# EN

# Annex VI

# Horizon Europe

# Work Programme 2025

## *6. Civil Security for Society*

# Table of contents

# Introduction

Cluster 3 provides a research and innovation response to a context of rapidly changing threats and challenges to internal security, the security of citizens, critical infrastructure and the security of society as a whole. These threats are driven by geopolitical, technological and societal changes, including:

- Instability, hybrid threats and the resurgence of war on the European continent, in particular the Russian war against Ukraine, making urgent the need for civilian protection and resilience.
- Continued threat from terrorism and increased threat from organised crime.
- Potential for large-scale movements of people, whether as a result of war or of other drivers, or the instrumentalisation of migration, requiring border management capabilities and a fight against migrant smuggling.
- More frequent and more serious climate-related extreme events as well as other disasters, whether accidental or intentional, of human or natural origin, requiring disaster risk management and response.
- Continued technological development and digitalisation create new and unforeseen vulnerabilities and new opportunities for criminals and violent extremists, as well as new challenges, needs and opportunities for security practitioners.
- Cyber threats that put infrastructures, businesses and individuals at risk.
- Negative socio-economic trends and climate adaptation that create potential for greater social polarisation and mistrust, which may escalate into conflict and/or create opportunities for extremists and malicious actors to spread hate speech and disinformation.

In addressing these and related challenges, this Work Programme will support the implementation of the EU Security Union Strategy[1] for the period for 2020 to 2025 and the sectoral strategies, legislation and action plans identified in the introduction to each of the **six Destinations**:

- **Better protect the EU and its citizens against Crime and Terrorism (FCT)**

*Link to the Horizon Europe Strategic Plan 2025-2027:* Expected impact 13 “Tackling crime and terrorism more effectively and increasing the resilience of infrastructures”.

- **Effective management of EU external borders (BM)**

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605

*Link to the Horizon Europe Strategic Plan 2025-2027:* Expected impact 12 "Facilitating legitimate movement of passengers and goods into the EU, while preventing illicit acts".

- **Resilient infrastructure (INFRA)**

*Link to the Horizon Europe Strategic Plan 2025-2027:* Expected impact 13 "Tackling crime and terrorism more effectively and increasing the resilience of infrastructures".

- **Increased Cybersecurity (CS)**

*Link to the Horizon Europe Strategic Plan 2025-2027:* Expected impact 14 "Increasing cybersecurity and making the online environment more secure".

- **Disaster-Resilient Society for Europe (DRS)**

*Link to the Horizon Europe Strategic Plan 2025-2027:* Expected impact 11. "Reducing losses from natural, accidental and human-made disasters".

- **Strengthened Security Research and Innovation (SSRI)**

*Link to the Horizon Europe Strategic Plan 2025-2027:* Cross-cutting Destination that supports all the Expected impacts identified above.

Each Destination includes an introductory section that explains the relevant policy objectives, that specifies any elements to be taken into account for the topics of the Destination and that identifies specific expected impacts. Proposals should set out a credible pathway to contributing to those specific expected impacts.

Successful projects need to show their understanding of and contribution to a wider innovation cycle based on a needs-driven capability development approach that triggers research, steers its implementation and capitalises on its outcomes. This means that projects need to show, on the one hand, an understanding of the capability requirement and policy context that has led to the R&I need, and, on the other hand, a strategy for ensuring the uptake of the outcomes including opportunities where relevant for using EU funds for deployment.

**Cross-cutting themes**

Various themes run through this Work Programme, cutting across the different sectoral Destinations. A first set of themes respond to the wider challenges identified in the three key strategic orientations of the Horizon Europe Strategic Plan 2025-2027:

- *Strengthening resilient societies and democracy*. The central focus of Cluster 3 is supporting the prevention, preparedness and response to the wide range of threats to internal security identified above, as well as ensuring the security of citizens, critical infrastructure and of society as a whole. Strengthening our democracies and making them more resilient – both materially and psychologically – has taken on a new urgency since the Russian invasion of Ukraine. European citizens need to be protected from hybrid threats such as disinformation campaigns or fake news while upholding the rule

of law and basic freedoms, including freedom of speech. Civil security research and innovation needs to equip civil security practitioners to mitigate the consequences of armed conflict, in particular attacks on critical infrastructures. By funding research to strengthen our societies and democracies against hybrid threats while protecting our infrastructures against cyber-physical attacks and preparing our societies and people, Cluster 3 shows its ability to adapt to changing conditions and challenges.

- *Securing the digital transition*. The more widespread and ubiquitous digital technology is, the greater the threats of new and unforeseen vulnerabilities and new opportunities for criminals and violent extremists as well as new challenges, needs and tools for law enforcement authorities, infrastructures, businesses and individuals. Research on cybercrime and cybersecurity helps to address these matters. With the aim of creating a secure and trustworthy digital environment Cluster 3 will invest in cybersecurity R&I to strengthen the EU's resilience, protect its infrastructures, and improve its ability to cope with cyber incidents. This will help increase the EU's open strategic autonomy in cybersecurity. Cluster 3 addresses cybercrime and the developing security threats in a digital age, such as criminal use of AI, to protect people, institutions and companies against cyber-enabled crimes. It will also continue to harness the opportunities of new technologies for law enforcement, border management and disaster risk reduction, and uphold the ability of the law enforcement to lawfully access and exploit digital evidence, without compromising or weakening privacy safeguards or cybersecurity (where relevant).

- *Supporting the green transition in civil security*. Climate change and environmental degradation are increasingly recognised as threat multipliers. Climate-related extreme events such as floods, droughts and forest fires pose increasing threats to people, nature business and infrastructure. Geological hazards such as earthquakes, volcanic eruptions, and tsunamis are also threats affecting security. As EU Member States and Associated Countries face similar challenges, with disasters of changing types and surpassing national borders, Cluster 3 will develop solutions to be applied throughout the EU to keep up to date with the developments. Cluster 3 will also address environmental crime. It will help understand how to manage borders in case of potential large-scale movements of people, including those caused by environmental stress. It will promote environmental sustainability of security solutions.

A second set of cross-cutting themes respond to challenges more specific to Cluster 3:

- *Ensuring legal and ethical outcomes that are supported by society*. Ethics, respect for the rule of law, fundamental rights, including human rights, privacy and the protection of personal data, as well as responsible research, must be at the heart of security research. Citizens and communities should be engaged, for example in assessing the societal impact of security technologies, to improve the quality of results and to build public trust. Social sciences and humanities (SSH) and social innovation need to be appropriately integrated into security research. The aim is to develop civilian security

solutions that are as little intrusive as possible while best respecting freedoms, rights and values.

- *Protecting and empowering the vulnerable*. Some people are more exposed to certain threats towards their security and well-being than others. These can be groups suffering from inequalities such as women, LGBTQI and children, who are more often exposed to certain types of violence than the average population. People depending on medicine are very vulnerable if supply chains are not secure, whether due to disasters or criminal activities. The needs and rights of travellers and migrants must be protected and promoted in border management activities. Vulnerable groups are more at risk of falling victims of trafficking in human beings. Research under Cluster 3 needs to consider how these groups can be better protected, including on the one hand by analysing the structures that foster violence against these groups and developing measures to tackle violence, and on the other hand by creating knowledge among the vulnerable groups themselves and empowering them to defend themselves.

- *Improving market uptake of civil security research solutions*. Despite many success stories of tools and capabilities used by security practitioners originating from EU-funded security research projects, the uptake and deployment of successful research results remains a constant challenge. This challenge spans all destinations of Cluster 3. This Work Programme:

    - continues the Cluster 3 practice of requiring projects to involve security practitioners alongside researchers and industry. Such involvement has shown its added value in ensuring that tools, technologies and capabilities are developed for the benefit of end-users and practitioners that can use them in their day-to-day work;

    - strengthens this involvement by introducing in many topics a requirement pursuant to which proposals should plan a mid-term deliverable consisting in the assessment, by the practitioners involved in the project, of the project's mid-term outcomes;

    - innovation procurement is used under the SSRI destination, this year with the open grounds preparatory work for future Pre-Commercial Procurement (PCP) topic, to bridge the gap between research, innovation and deployment, and in so doing also to strengthen the European market and European civil security industrial base;

    - encourages synergies with other EU funding programmes and instruments to enable or facilitate the uptake of the results of research into deployable solutions. Further information about this is given below.

    - the possibilities and support of security end-users like FRONTEX, EUROPOL, EU-LISA and the EU Drug Agency, for testing and validation of security research results should be used and expanded to the fullest extent.

- supports projects which can directly or indirectly support public institutions intent on setting up their own innovation processes, which is to be encouraged.

Where relevant Cluster 3 will make use of space technology and Earth Observation.

**International cooperation**

For the purposes of this Work Programme, entities established in Horizon Europe Associated Countries will be treated as entities established within the EU.

Beyond that, Cluster 3 continues to require a specific approach to international cooperation to achieve the right balance between the benefits of exchange with key international partners, while at the same time ensuring the protection of the EU's security interests and the need for open strategic autonomy in critical sectors.

Under the destination 'Disaster-Resilient Society for Europe' (DRS), there is an established culture of comprehensive research collaboration with non-EU countries, taking account of the transnational aspect of different natural and human-made hazards and their causes (such as climate change). Therefore, under this destination, international cooperation is strongly encouraged, given the value of cooperating internationally, in particular in developing technologies for first responders to use.

For the destinations relating to border management, the fight against crime and terrorism, infrastructure resilience and cybersecurity, international cooperation will be explicitly encouraged only where appropriate and specifically supportive of ongoing collaborative activities.

**Synergies with other EU funding programmes and instruments**

Cluster 3 will continue building and facilitating synergies with other EU funding programmes and instruments, in an approach with long-term capability development planning at its core. This is particularly important for civil security, where solutions are often demand-driven in a market that tends to be narrow, institutional, highly regulated, sensitive, and often fragmented along national lines.

From the demand side (funding for security practitioners and authorities, who are the users of security solutions), Cluster 3 will continue to operationalise the synergies with the home affairs funds: the Internal Security Fund (ISF) and the Integrated Border Management Fund (IBMF) in its two components, the Border Management and Visa Instrument (BMVI) and the Customs Control Equipment Instrument (CCEI), as well with other funds such as the ECHO Enhanced Response Capacity (ERC) funds. This will mean both facilitating the uptake of the results of Cluster 3 research by Member States and Associated Countries in their national programmes, and programming EU and specific actions with funding dedicated to taking up innovation resulting from Cluster 3 research.

In addition to the home affairs funds, Cluster 3 will continue promoting synergies with the Digital Europe Programme, the European Maritime Fisheries and Aquaculture Fund

(EMFAF), the Union Civil Protection Mechanism (Knowledge for Action in Prevention and Preparedness calls for proposals, rescEU grants, early warning capabilities, and the training and exercises programme), the European Regional Development Fund (ERDF), the Cohesion Fund, the Neighbourhood, Development and International Cooperation Instrument – Global Europe instrument for the Southern and Eastern Neighbourhood and the Instrument for Pre-Accession, the Technical Support Instrument (TSI), the OLAF Union Anti-Fraud Programme (UAFP) and EU4Health.

From the supply side (funding for European innovators who develop and commercialise security solutions), the promotion of the uptake of the results of Cluster 3 research could involve the Innovation Fund and, to a lesser extent, EU actions under the ISF and the BMVI, as well as Health Emergency Preparedness and Response HERA Invest.

Practical ways in which Cluster 3 will continue to improve and promote synergies include raising Member States' and Associated Countries authorities' and innovators' awareness of the opportunities for funding for uptake in other EU programmes and instruments; tracking and studying uptake of Cluster 3 projects' results in other EU programmes and instruments; planning actions in other EU funding programmes and instruments to fund innovation in civil security that takes up the results of Cluster 3 research.

Research funded under Cluster 3 will continue to focus exclusively on civilian applications. Coordination with the European Defence Fund (EDF) and the EU Space Programme will be sought in order to strengthen cross-cluster complementarities also with actions foreseen in Cluster 4[2].

**Implementation**

The provision of Financial Support to Third Parties by successful projects is mandatory for four topics in this Work Programme. The eligibility for Financial Support to Third Parties is limited to entities established in EU Member States and to Associated Countries. Further conditions apply.

[2] To this end, the Commission and Member States have in place a mechanism for strategic planning and coordination of R&D related to the Copernicus Security Services (CSS), which maps current operational services and on-going and planned R&D initiatives, as well as it identifies end-user operational requirements and promotes sharing of information between projects with common interests. The mechanism drives R&D objectives listed in a Strategic Research Agenda (SRA) updated on a yearly basis. Engagement in the CSS-SRA information sharing process is therefore sought, for those projects planning to use Earth Observation and associated services for civil security applications.

# Calls

## Call - HORIZON-CL3-2025-01 Civil Security for Society

***HORIZON-CL3-2025-01***

### Overview of this call[3]

Proposals are invited against the following Destinations and topic(s):

| Topics | Type of Action | Budgets (EUR million) | Expected EU contribution per project (EUR million)[4] | Indicative number of projects expected to be funded |
|---|---|---|---|---|
| | | 2025 | | |
| Opening: 12 Jun 2025<br>Deadline(s): 12 Nov 2025 | | | | |
| Destination - Better protect the EU and its citizens against Crime and Terrorism | | | | |
| HORIZON-CL3-2025-01-FCT-01: Open topic on modern information and forensic evidence analysis and on frontline policing | RIA | 18.00 | Around 3.00 | 6 |
| HORIZON-CL3-2025-01-FCT-02: Open topic on prevention, detection and deterrence of various forms of crime and terrorism through an enhanced understanding of the related societal issues | RIA | 12.00 | Around 3.00 | 4 |
| HORIZON-CL3-2025-01-FCT-03: Open topic on improved intelligence picture and enhanced prevention, detection and deterrence of various forms of organised crime | IA | 8.00 | Around 4.00 | 2 |

[3] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for 2025.

[4] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

| | | | | |
|---|---|---|---|---|
| Destination - Effective management of EU external borders | | | | |
| HORIZON-CL3-2025-01-BM-01: Open topic on efficient border surveillance and maritime security | IA | 10.50 | Around 3.50 | 3 |
| HORIZON-CL3-2025-01-BM-02: Open topic on secured and facilitated crossing of external borders | RIA | 9.00 | Around 3.00 | 3 |
| HORIZON-CL3-2025-01-BM-03: Open topic on better customs and supply chain security | IA | 9.00 | Around 3.00 | 3 |
| Destination - Resilient Infrastructure | | | | |
| HORIZON-CL3-2025-01-INFRA-01: Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures | IA | 15.00 | Around 5.00 | 3 |
| HORIZON-CL3-2025-01-INFRA-02: Open topic for role of the human factor for the resilience of critical infrastructures | RIA | 7.00 | Around 3.50 | 2 |

| | | | | |
|---|---|---|---|---|
| Destination - Disaster-Resilient Society for Europe | | | | |
| HORIZON-CL3-2025-01-DRS-01: Open topic on citizen and regional and/or local authorities' engagement in enhanced disaster risk awareness, including education, and preparedness | RIA | 12.00 | Around 4.00 | 3 |
| HORIZON-CL3-2025-01-DRS-02: Open topic on Improving disaster risk management and governance to ensure self-sufficiency and sustainability of operations in support of enhanced resilience | RIA | 10.50 | Around 3.50 | 3 |
| HORIZON-CL3-2025-01-DRS-03: Open topic on Testing / validating tools, technologies and data used in cross-border prevention, preparedness and responses to climate extreme and geological events and chemical, biological or | IA | 13.50 | Around 4.50 | 3 |

| | | | | |
|---|---|---|---|---|
| radiological emergency threats | | | | |
| Destination - Strengthened Security Research and Innovation | | | | |
| HORIZON-CL3-2025-01-SSRI-01: National Contact Points (NCPs) in the field of security and cybersecurity fostering the links with National Community building for Safe, Secure and Resilient Societies | CSA | 3.00 | Around 3.00 | 1 |
| HORIZON-CL3-2025-01-SSRI-02: Uptake Acceleration Services | CSA | 5.00 | Around 5.00 | 1 |
| HORIZON-CL3-2025-01-SSRI-03: Open grounds for pre-commercial procurement of innovative security technologies | CSA | 2.00 | Around 1.00 | 2 |
| HORIZON-CL3-2025-01-SSRI-04: Accelerating uptake through open proposals for advanced SME innovation Specific conditions | IA | 3.00 | Around 1.50 | 2 |
| HORIZON-CL3-2025-01-SSRI-05: Data repository for security research and innovation | IA | 3.00 | Around 3.00 | 1 |
| Overall indicative budget | | 140.50 | | |

| **General conditions relating to this call** | |
|---|---|
| *Admissibility conditions* | The conditions are described in General Annex A. |
| *Eligibility conditions* | The conditions are described in General Annex B. |
| *Financial and operational capacity and exclusion* | The criteria are described in General Annex C. |
| *Award criteria* | The criteria are described in General Annex D. |
| *Documents* | The documents are described in General Annex E. |

| | |
|---|---|
| *Procedure* | The procedure is described in General Annex F. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. |

## Call - HORIZON-CL3-2025-02 Civil Security for Society

***HORIZON-CL3-2025-02***

### Overview of this call[5]

Proposals are invited against the following Destinations and topic(s):

| Topics | Type of Action | Budgets (EUR million) 2025 | Expected EU contribution per project (EUR million)[6] | Indicative number of projects expected to be funded |
|---|---|---|---|---|
| Opening: 12 Jun 2025<br>Deadline(s): 12 Nov 2025 | | | | |
| Destination - Increased Cybersecurity | | | | |
| HORIZON-CL3-2025-02-CS-01: Generative AI for Cybersecurity applications | RIA | 44.00 | 14.00 to 16.00 | 3 |
| HORIZON-CL3-2025-02-CS-02: New advanced tools and processes for Operational Cybersecurity | IA | 25.55 | 4.50 to 6.00 | 5 |
| HORIZON-CL3-2025-02-CS-03: Privacy Enhancing Technologies | IA | 11.00 | 3.00 to 4.00 | 3 |
| HORIZON-CL3-2025-02-CS-04: Security of Post- | IA | 4.00 | 1.00 to | 2 |

5 The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for 2025.

6 Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

| | | | | | |
|---|---|---|---|---|---|
| Quantum primitives | | | | 2.00 | |
| HORIZON-CL3-2025-02-CS-05: Security of implementations of Post-Quantum Cryptography algorithms | IA | 6.00 | 1.00 to 2.00 | | 3 |
| Overall indicative budget | | 90.55 | | | |

| **General conditions relating to this call** | |
|---|---|
| *Admissibility conditions* | The conditions are described in General Annex A. |
| *Eligibility conditions* | The conditions are described in General Annex B. |
| *Financial and operational capacity and exclusion* | The criteria are described in General Annex C. |
| *Award criteria* | The criteria are described in General Annex D. |
| *Documents* | The documents are described in General Annex E. |
| *Procedure* | The procedure is described in General Annex F. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. |

# Destinations

## Destination - Better protect the EU and its citizens against Crime and Terrorism

As underlined in the Horizon Europe Strategic Plan 2025-2027, proposals for topics under this Destination should "*continue developing European practitioners' capabilities to effectively prevent, detect and investigate terrorism, organised crime [...], cybercrime, the most harmful crimes [...] and criminal aspects of behaviour on the internet [...]. Investment provides further support for modern information analysis, modern forensics tools [...], lawful evidence collection, and the recognition of societal problems arising from various forms of crime. This destination will also prepare policymakers, practitioners, companies and the general public for tackling emerging and evolving threats, by identifying them early on, flagging them and making preliminary recommendations on how to deal with them. Areas of new or increased focus will include the identification and investigation of criminal networks including emerging phenomena [...]. The destination will continue to pay close attention to financial crimes, as a common denominator for most criminal activities*." To this end, proposals should contribute to the achievement of one or more of the following impacts:

- Modern information analysis for Police Authorities, allowing them to efficiently fight criminals and terrorists who use novel technologies;
- Improved forensics and lawful evidence collection, increasing the capabilities to apprehend criminals and terrorists and bring them to the court;
- Enhanced prevention, detection and deterrence of societal issues related to various forms of crime, including cybercrime, and terrorism, such as violent radicalisation, domestic and sexual violence, including child sexual abuse, or juvenile offenders;
- Increased security of citizens against terrorism, including in public spaces (while preserving their quality and openness);
- Improved intelligence picture and enhanced prevention, detection and deterrence of various forms of organised crime;
- More secure cyberspace for citizens, especially children, through a robust prevention, detection, and protection from cybercriminal activities.

More specifically, in the rapidly evolving technological and societal landscape, with climate change and environmental aspects increasingly seen as security issues, and with growing threats to vulnerable citizens, various forthcoming challenges that European society faces deserve dedicated research and innovation actions in the scope of this Destination. Some of them are:

- Challenges related to modern information and forensic evidence analysis as well as to frontline policing, such as

- criminal use of various forms of cutting-edge technologies,
- development of novel methods of forensics analysis based on new and emerging technologies, e.g., forensic on-site analysis with mobile real-time cloud sharing applications,
- lawful access to and integrity of data and evidence, or
- modern physical threats to frontline police and corresponding needs for a next generation smart police protective gear;

- Challenges regarding prevention, detection and deterrence of various forms of crime and terrorism through an enhanced understanding of the related societal issues, in the context of:
  - crime, such as
    - vulnerability of children and youth, both offline and online,
    - increased availability and use of stimulants and synthetic drugs, or
    - forest fires of criminal origin;
  - terrorism and radicalisation, such as
    - blurring of lines between different types of terrorism, including right-wing, left-wing, anarchist, jihadist, and other ideologies, or
    - expansion of lone actors' attacks in the background of social isolation, polarisation and recurrent economic crises;
    - multiplication of non-violent forms of radicalisation, such as malign foreign influences and funding aimed at challenging and undermining EU values.
- Challenges related to improving the intelligence picture and enhancing the prevention, detection and deterrence of various forms of organised crime, such as
  - organised criminal groups profiting from migrant smuggling and trafficking in human beings;
  - drug-related violence and the association between involvement in the drug market with other forms of criminality and violent crime.

Research and innovation funded under this Destination will contribute to policy objectives such as those of the:

- Police cooperation package[7] (information exchange, automated data exchange for police cooperation - "Prüm II", operational cross-border police cooperation);
- Counter-Terrorism Agenda for the EU[8] (incl. Regulation 2021/784/EU on addressing dissemination of terrorist content online & Directive 2017/541/EU on combating terrorism);
- EU C-UAS Strategy[9] (counter-drone policy);
- EU Strategy to Tackle Organised crime[10];
- EU Strategy on combatting Trafficking in Human Beings[11] (the modified Directive on preventing and combating trafficking in human being and protecting its victims), and the Proposal to strengthen EU legislation to prevent and fight migrant smuggling (notably its aspect of reinforcing Europol's role in the fight against migrant smuggling and trafficking in human beings);
- EU drugs measures[12] (Strategy, Action Plan and Roadmap to fight Drugs Trafficking and Organised Crime);
- EU environmental crime measures[13] (review of the Directive 2008/99/EC on protection of the environment through criminal law);
- EU anti-corruption measures[14] (Communication, proposal for a Directive);
- Directive (EU) 2019/713 on non-cash means of payment;
- EU strategy on a more effective fight against child sexual abuse[15] (incl. Proposal for a regulation to prevent and combat child sexual abuse); and
- EU Regulation (2022/2371) on serious cross-border threats to health.

This Destination will also support, whenever appropriate and applicable, proposals with:

- a clear strategy on how they will adapt to the fast-evolving environment in the area of fight against crime and terrorism (evolution of related technologies, evolution of criminal modi operandi and business models related to these technologies, etc.);
- the involvement of Police Authorities in their core;

7 COM/2021/782 final, COM/2021/784 final, ST/8720/2022/INIT.
8 COM/2020/795 final.
9 COM/2023/659 final.COM/2023/659 final.
10 COM/2021/170 final.
11 COM/2021/171 final; COM/2022/732 final; COM/2023/755 final; COM/2023/754 final.
12 14178/20; ST/9819/2021/INIT; COM/2023/641 final.
13 16069/23.
14 JOIN(2023) 12 final; COM/2023/234 final.
15 COM/2020/607 final; COM/2022/209 final.

- the active role for Non-Governmental Organisations (NGOs) and Civil Society Organisations (CSOs);
- the active involvement of Small and Medium Enterprises (SMEs);
- a minimum-needed platform, i.e., tools that are modular and can be easily plugged into another platform (in order to avoid platform multiplication) ;
- tools that are developed and validated against practitioners' needs and requirements;
- a robust plan on how they will build on the relevant predecessor projects;
- education and training aspects, especially for Police Authorities and other relevant practitioners, as well as information sharing and awareness raising of the citizens;
- a clear strategy on the uptake of the outcomes, defined in consultation with the involved stakeholders and theirsustainability;
- a well-developed plan both on how research data for training and testing will be obtained, in order to reach the requested Technology Readiness Levels (TRLs), and on how the specific TRL will be measured.

Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, in coordination with the Community for European Research and Innovation for Security (CERIS).

Proposals are invited against the following topic(s):

**HORIZON-CL3-2025-01-FCT-01: Open topic on modern information and forensic evidence analysis and on frontline policing**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 18.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply: |

| | |
|---|---|
| | This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities [16] from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br><br>To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one project that is the highest ranked within each of the three options (Option a), Option b) and Option c)), provided that the applications attain all thresholds.<br><br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to some or all of the following expected outcomes:

- Modern, uniform and validated tools, skills, methodologies and innovative training curricula for security practitioners (European Police Authorities, forensic institutes) to prevent, detect and investigate criminal and terrorist offences, including the lawful court-proof collection of crime evidence;
- Improved mechanisms for cross-border information exchange in the fight against crime and terrorism, taking into account all applicable legislation and fundamental rights;
- Evidence-based support to policy-makers on shaping and tuning of regulation related to modern information analysis, forensic evidence analysis or frontline policing.

Scope: Under the Open Topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for improving modern information and forensic evidence analysis or frontline policing, that are not covered by topics

[16] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

of Horizon Europe Calls Fighting Crime and Terrorism 2023-2024. If they relate to some of the topics covered by Horizon Europe Calls Fighting Crime and Terrorism 2021-2022, the proposals should convincingly explain how they will build on and not duplicate them.

Proposals are expected to address one of the following options:

**Option a**: tackling advanced technology challenges;

**Option b**: modern forensics analysis using new and emerging technologies;

**Option c**: modernisation of frontline policing.

Adapted to the nature, scope and type of proposed projects, proposals should also convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Furthermore, proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on if appropriate and not duplicate previous research, including but not limited to research by other Framework Programmes' projects.

Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. For Option b), the active involvement, as beneficiaries, of forensic institutes from EU Member States or Associated Countries is recommended.

Proposals funded under this topic are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. Similarly, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes.

In order to ensure the active involvement of and timely feedback from relevant security practitioners, i.e., Police Authorities and/or forensic institutes, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

**HORIZON-CL3-2025-01-FCT-02: Open topic on prevention, detection and deterrence of various forms of crime and terrorism through an enhanced understanding of the related societal issues**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** |
|---|
| **Specific conditions** |

| | |
|---|---|
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 12.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 1 Police Authority[17] and at least 1 Civil Society Organisation, CSO (or Non-Governmental Organisation, NGO) from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one project that is the highest ranked within each of the two options (Option a and Option b), provided that the applications attain all thresholds.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Beneficiaries should provide financial support to third parties in the form of grants. The maximum amount to be granted to each third party is EUR 60 000 to support effective collaboration and/or coordination with additional relevant national Police Authorities and/or CSOs/NGOs from EU Member States or Associated Countries. |

[17] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

| | |
|---|---|
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to some or all of the following expected outcomes:

- Improved, modern, uniform and validated tools, skills or methodologies as well as innovative training curricula for security practitioners (European Police Authorities, Non-Governmental Organisations, Civil Society Organisations) to prevent, detect and deter criminal or terrorist offences, taking into account all applicable legislation and fundamental rights;
- Enhanced understanding of the cultural and societal aspects of crime or terrorism/radicalisation, as well as on the key challenges related to combating them;
- Evidence-based support to policymakers on shaping and tuning of regulation related to crime or terrorism/radicalisation;
- Enhanced perception by citizens that Europe is an area of freedom, justice, security and respect of privacy and human rights, thanks to, e.g., innovative awareness-raising campaigns explaining to citizens the key and evolving mechanisms of crime or terrorism/radicalisation, and how to protect against them.

Scope: Under the Open Topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for improving the prevention, detection and deterrence of various forms of crime or terrorism/radicalisation through an enhanced understanding of the related societal issues. These challenges and/or solutions should not be covered by topics of Horizon Europe Calls Fighting Crime and Terrorism 2023-2024. If they relate to some of the topics covered by Horizon Europe Calls Fighting Crime and Terrorism 2021-2022, the proposals should convincingly explain how they will build on and not duplicate them. The same applies regarding Horizon Europe projects under the calls HORIZON-CL2-2022-DEMOCRACY-01-05: Evolution of political extremism, and HORIZON-CL2-2024-DEMOCRACY-01-05: Gender-roles in extremist movements.

Proposals are expected to address one of the following options:

**Option a**: societal issues related to crime;

**Option b**: societal issues related to terrorism and radicalisation.

Adapted to the nature, scope and type of proposed projects, proposals should also convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Furthermore, proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on if appropriate and not duplicate

previous research, including but not limited to research by other Framework Programmes' projects.

Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

Proposals funded under this topic are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. Similarly, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes.

If the funded proposal concerns radicalisation, the consortium is encouraged to liaise with the EU Knowledge Hub on prevention of radicalisation with the aim of facilitating the streamlining of their priorities and the dissemination of their results.

In order to ensure the active involvement of and timely feedback from relevant security practitioners, i.e., Police Authorities and Non-Governmental Organisations / Civil Society Organisations, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project.

Activities proposed within this topic should address both technological and societal dimensions of the tackled challenge in a balanced way. This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related innovation activities.

Proposals should plan their activities opting for the Financial Support to Third Parties in order to provide financial support to practitioners (Police Authorities and/or Non-Governmental Organisations/Civil Society Organisations) for expanding the proposed work in terms of additional user groups, complementary assessments, technology- or methodology-testing activities. in line with the conditions set out in Part B of the General Annexes. Each consortium will define the selection process of the third parties for which financial support will be granted . From 5% up to 20% of the EU funding requested by the proposal may be allocated to the purpose of financial support to third parties.

**HORIZON-CL3-2025-01-FCT-03: Open topic on improved intelligence picture and enhanced prevention, detection and deterrence of various forms of organised crime**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal |

| | |
|---|---|
| *project* | requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 8.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [18] from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to all of the following expected outcomes:

- Improved, modern, uniform and validated tools, skills, methodologies and innovative training curricula for European Police Authorities to prevent, detect and investigate organised crime offences, including the early detection of criminal networks and of the emerging trends and challenges;

- Improved mechanisms for the use of cross-border tools to facilitate secure information exchange in the fight against organised crime, including criminal networks, taking into account all applicable legislation and fundamental rights;

[18] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

- Enhanced understanding of the key challenges and best practices related to combating cross-border organised crime;

- Evidence-based support to policy-makers on shaping and tuning of regulation related to cross-border organised crime including criminal networks.

Scope: Under the Open Topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for improving the intelligence picture and enhancing the prevention, detection and deterrence of various forms of organised crime, that are not covered by topics of Horizon Europe Calls Fighting Crime and Terrorism 2023-2024. If they related to some of the topics covered by Horizon Europe Calls Fighting Crime and Terrorism 2021-2022, the proposals should convincingly explain how they will build on and not duplicate them. Adapted to the nature, scope and type of proposed projects, proposals should also convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Furthermore, proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on if appropriate and not duplicate previous research, including but not limited to research by other Framework Programmes' projects.

Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact. If relevant, the active involvement, as beneficiaries, of Border Guard and/or Customs Authorities from EU Member States or Associated Countries is recommended.

Proposals funded under this topic are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. Similarly, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes.

In order to ensure the active involvement of and timely feedback from relevant security practitioners, i.e., Police Authorities and Border Guards / Customs Authorities, proposals should plan a mid-term deliverable consisting in the assessment, performed by the practitioners involved in the project, of the project's mid-term outcomes.

In this topic, the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

**Destination - Effective management of EU external borders**

Proposals for topics under this Destination should contribute to the following expected impact: "facilitating legitimate movement of passengers and goods into the EU, while preventing illicit acts" of the Horizon Europe Strategic Plan 2025-2027.

Projects funded under the topics of Work Programme 2025 will promote technological and social research and innovation and further explore and develop future capabilities for European practitioners in the areas of border management, customs and supply chain security, and civilian maritime security. Capability areas to address may include:

- monitoring, preparedness and reaction in border management tasks, managing irregular or illegal activities involving people or goods across external borders of the EU;
- safeguarding human rights, and ensuring legal compliance, in efficient border management;
- integrated and continuous border surveillance, situational awareness (including but not limiting to maritime situational awareness) and analysis support;
- safety, user experience and performance of practitioners' staff in border management;
- security, privacy and usability of identity and (travel) documents;
- facilitating travel of bona fide passengers across external borders of the EU;
- data analysis on documents, biometrics, or cargo compliant with GDPR[19] and EU Artificial Intelligence Act[20] and compatible with sandboxes approaches;
- detection of dangerous, illicit and illegal goods and materials trafficked through external borders of the EU and the supply chain;
- prevention and disruption of such trafficking.

Research and innovation funded under this Destination will contribute to policy objectives such as:

- the border management and security dimensions of the Pact on Migration and Asylum[21];
- the Multiannual Strategic Policy for European Integrated Border Management[22];
- the Capability Roadmap of the European Border and Coast Guard[23];
- the proposals to strengthen EU legislation to prevent and fight migrant smuggling[24];

19 Regulation (EU) 2016/679.
20 2021/0106(COD).
21 COM (2020) 610 final.
22 COM (2023) 146 final.
23 FRONTEX MB Decision 16/2024.

- the proposals on digitalisation of travel documents and facilitation of travel[25];
- the civil security aspects of the updated EU Maritime Security Strategy[26];
- the proposals for EU Customs reform[27].

Research and innovation will contribute to sustain and improve capabilities to cope with potential future critical situations or emerging challenges regarding both the flow of people and the flow of goods across external EU borders. Examples may include:

- threats of illicit flows of dangerous materials and weapons because of conflicts outside the Union;
- the potential for large-scale movements of people including those resulting from the instrumentalisation of irregular migration, from conflicts, or from social, economic, environmental and climate stress in the EU neighbourhood;
- the exploitation and smuggling of migrants across the EU's external borders, in particular of vulnerable groups including women and girls.

Furthermore, challenges can be exacerbated by the rapid adoption of new technologies by criminal organisations, and how new technologies help the sophistication of organised crime methods.

Among technological approaches, for example, artificial intelligence (AI) offers many opportunities to improve border management services, including analytical support. At the same time AI also brings challenges such as morphing; potential misuse of data; doubts of bias or unexplained decision supports. Research and innovation are also necessary to minimise risks from these challenges, also in light of the full entry into force of the EU Artificial Intelligence Act.

Furthermore, research and innovation under this Destination will contribute to:

- lower the environmental impact and footprint of border, customs and supply chain security tasks, through innovative solutions and methods;
- integrate and improve safety and cybersecurity of EU information systems, of innovative equipment, and of information and data in these areas, especially during their exchange at operational or tactical levels;

---

24 COM/2023/754 final; COM/2023/755 final.
25 COM (2021) 277 final.
26 11205/14.
27 COM (2023) 257 final; COM (2023) 258 final – 2023/0156(COD); COM (2023) 259 final – 2023/0157(NLE); COM (2023) 262 final – 2023/0158(CNS).

- safeguard the open strategic autonomy and technological sovereignty of the EU in critical security areas by contributing to a more competitive and resilient EU security technology and industrial base.

Research projects funded under this Destination should engage with all stakeholders involved, including travellers, migrants, and operators, as relevant. Research will integrate approaches to safeguarding and promoting EU values and fundamental rights in these areas, with a special focus on human rights.

Projects should align and contribute to the realisation of the Capability Roadmap of the European Border and Coast Guard (EBCG) published by the EBCG Agency (Frontex), especially the Roadmap's mid- and long-term perspectives. The Roadmap provides strategic vision for investments into the development of capabilities and is the result of integrated planning between the Member States and the European Border and Coast Guard Agency. Proposals submitted under this Destination should explain the alignment with the Capability Roadmap and the plans for further uptake of the research outcomes, especially by involved practitioners in line with their national Capability Development Plans.

Frontex will be closely associated with and will assist Member States and the European Commission in drawing up and implementing relevant research and innovation activities. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) may also assist the European Commission on relevant research and innovation activities and specific topics. Hence proposals should consider and foresee that Frontex and/or eu-LISA may for example observe projects' pilots and demonstrations, with the aim of facilitating future uptake of innovations for the border and coast guard community. Furthermore, funded projects will likely have the opportunity of exploiting the core capabilities of the "Frontex Technology and Innovation Centre", Frontex's future collaborative space for testing, demonstration, simulation and assessment of solutions, processes and procedures.

To accomplish the objectives of this Destination, additional eligibility conditions have been defined regarding the active involvement of relevant security practitioners or end-users in the research projects' Consortia.

Proposals submitted under this Destination should demonstrate how they plan to build on relevant predecessor projects; to consider the citizens' and societal perspectives; to include education, training and awareness raising for practitioners and citizens; to measure the achieved TRL.

Regarding synergies and complementarities, this Destination will develop knowledge and technologies that may be taken up by other instruments, such as the Integrated Border Management Fund, in its components of the Border Management and Visa Instrument (BMVI) and Customs Control Equipment Instrument (CCEI). Member States authorities participating in research projects can plan to use those instruments for uptake (piloting, testing, validation, scale-up, transfer, acquire, deploy, etc) of innovative solutions developed from research, as early as TRL 7.

Cluster 3 will further incentivise the use of European Space Programmes' services for border management innovation where relevant and their services and capabilities, including demonstration and validation of new technologies in operational environments.

Successful proposals under this Destination are invited to cooperate with other EU-led or EU-funded initiatives in the relevant domains, such as the Knowledge Networks for Security Research & Innovation funded under Horizon Europe Cluster 3, or other security research and innovation working groups set-up by the Commission or EU Agencies.

Where possible and relevant, synergy-building and clustering initiatives with projects in the same area should be considered, in coordination with the Community for European Research and Innovation (CERIS).

Proposals are invited against the following topic(s):

**HORIZON-CL3-2025-01-BM-01: Open topic on efficient border surveillance and maritime security**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 10.50 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Border or Coast Guard Authorities from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology* | Activities are expected to achieve TRL 6-7 by the end of the project – |

| | |
|---|---|
| *Readiness Level* | see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [28]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to all of the following expected outcome(s):

- Improved security of EU external borders, or of maritime environment, infrastructures and activities, against natural, accidental or incidental disasters; or disasters affecting the environments and security challenges such as illegal trafficking, irregular migration or exceptional situations of mass arrivals at external borders, illegal exploitation of natural resources, piracy and potential terrorist attacks, cyber and hybrid threats;
- Sustained and improved surveillance, real-time situational awareness, and reaction capabilities to cope with potential critical situations at the EU external borders;
- Improved capabilities for assessing, confirming and respond to distress situations at sea.

Scope: Under this topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for improving capabilities of practitioners in border surveillance and/or maritime security. External border areas, pre-frontier areas as well as contexts and scenarios in Europe's border regions that may in the future be impacted by geopolitical instabilities, hybrid threats, or tensions from outside the EU, and need sustained and improved surveillance and reaction capabilities, could be particularly considered. If they relate to some of the topics covered by Horizon Europe Calls Effective Management of EU External Borders 2021-2022 or 2023-2024, the proposals should convincingly explain how they will build on and not duplicate them.

[28] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

Proposals may also address capabilities of information exchange, capabilities for detection of illegal activities, and/or solutions that can be deployed efficiently across diverse geographical regions; capabilities for operational event data recording; capabilities to detect irregular activities in areas of terminals for travel (air, sea) or logistics terminals around a Border Control Point, without disrupting the flow of operations.

The EBCG Capability Roadmap recognises that future surveillance capabilities that help detect cross-border irregularities and cases requiring Search and Rescue activities are essential. Solutions should be modular and scalable to cater to the regional and challenges specificities.

Examples of technologies and solutions that may be relevant for this topic include but are not limited to: sensing (at tactical, operational, and/or strategic levels), autonomous platforms, , vehicles and systems (aerial, ground, surface or underwater, vessel-based or not, mobile or land-borne, etc); interconnectivity between sensors and platforms and automated data fusion; data processing systems; image processing; robotics; computing technologies including edge and cloud computing; human-machine interfaces.

Projects must integrate:

- perspectives of safeguarding and promoting human rights, developing solutions that contribute to those safeguarding and promotion;
- inputs from human rights, law and ethical perspectives, as well as the consideration and views of individuals and society, as well as a gender sensitive approach, as appropriate; proposals can engage with civil society organisations for wider input and support;
- aspects of cybersecurity of the technology proposed, and the protection of communication systems and networks involved in the solutions, if and as relevant.

Proposals that include solutions and/or methods that would contribute to a lower environmental impact and footprint, better cost-efficiency, better energy-efficiency, and/or better operational autonomy of the capabilities and solutions in this topic, would be welcome.

Depending on the particular scope of the proposal, participation of Police Authorities is welcome.

In order to ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project’s mid-term outcomes, performed by the practitioners involved in the project. .

In this topic, the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

## HORIZON-CL3-2025-01-BM-02: Open topic on secured and facilitated crossing of external borders

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 9.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Border or Coast Guard Authorities from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [29]. |

[29] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:

| | |
|---|---|
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to the following expected outcome(s):

- Improved border crossing experience for travellers and border authorities' staff (including customs, coast and border guards), while maintaining security and monitoring of movements across EU external borders, supporting the Schengen area, reducing illegal movements of people and goods across those borders and protecting fundamental rights of travellers, both EU citizens and Third Country Nationals.

Scope: Under this topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for improving capabilities of practitioners for the secured and facilitated checks of crossings of external borders. Contexts and scenarios in Europe's border regions that may in the future be impacted by geopolitical instabilities or tensions from outside the EU, and need sustained and improved surveillance and reaction capabilities, could be particularly considered. If they relate to some of the topics covered by Horizon Europe Calls Effective Management of EU External Borders 2021-2022 or 2023-2024, the proposals should convincingly explain how they will build on and not duplicate them.

Proposals may also address capabilities related to possible future digitalised travel credentials (DTC), including though not limited to: Type-1 and Type-2 and forward integration with secure digital citizenship wallet(s); identification and verification in the context of border checks; optimisation of resources in the context of border checks.

According to the EBCG Capability Roadmap, legal border crossings should be as swift and simple as possible, preferably fully automated. Border Crossing Points should also have the ability to detect any unauthorised crossings of persons or goods.

Examples of technologies and solutions that may be relevant for this topic include but are not limited to: secure and private data approaches for applications in border checks; fuzzy searches capabilities; data communication, translation and sharing solutions; biometrics; age assessment methods; fraudulent documents detection; automation, exchange and interoperability for systems involved in border checks.

Projects must integrate aspects of:

- perspectives of safeguarding and promoting human rights, developing solutions that contribute to those safeguarding and promotion;

---

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- inputs from human rights, law and ethical perspectives, as well as the consideration and views of individuals and society and the societal dimension, including a gender sensitive approach, as appropriate; proposals can engage with citizens and civil society for wider input and support;

- aspects of cybersecurity of the technology proposed, and the protection of communication systems and networks involved in the solutions, if and as relevant.

Proposals that include solutions and/or methods that would contribute to a lower environmental impact and footprint, better cost-efficiency, better energy-efficiency, and/or better operational autonomy of the capabilities and solutions in this topic, would be welcome.

Depending on the particular scope of the proposal, participation of Police Authorities is welcome.

In order to ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project.

**HORIZON-CL3-2025-01-BM-03: Open topic on better customs and supply chain security**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 9.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Customs Authorities from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of |

| | |
|---|---|
| | Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [30].<br>Beneficiaries should provide financial support to third parties in the form of grants. The maximum amount to be granted to each third party is EUR 100 000 to support effective collaboration and/or coordination with additional relevant national Customs Authorities, including testing and validation activities within the projects. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to the following expected outcome(s):

- Improved customs and supply chain security though better prevention, detection, deterrence and/or fight of illegal activities involving flows of goods across EU external borders and through the supply chain, and/or through better interoperability, minimising disruption to trade flows.

Scope: Under this topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for improving capabilities of practitioners for the security of customs and the supply chain. Contexts and scenarios in Europe's border regions that may in the future be impacted by geopolitical instabilities, tensions from outside the EU or impact on the environment, and need sustained and improved surveillance and reaction capabilities, could be particularly considered. If they relate to some of the topics covered by Horizon Europe Calls Effective Management of EU External Borders 2021-2022

[30] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

or 2023-2024, the proposals should convincingly explain how they will build on and not duplicate them.

Proposals may also address capabilities related to possible future detection of threats in the flow of goods and/or in the supply chain in a flexible, rapid, relocatable way. Detection capabilities could target one or more type(s) of dangerous, illicit and/or illegal goods or materials, including illicit drugs and their precursors, illegally traded CITES speciesalso considering the European Deforestation Free Products Regulation, contraband, CBRNE threats and/or various modi operandi related to cross-border trafficking, including involving cargo.

Projects must integrate aspects of:

- perspectives of safeguarding and promoting human rights, developing solutions that contribute to those safeguarding and promotion;
- inputs from human rights, law and ethical perspectives, as well as the consideration and views of individuals and society, as appropriate; proposals can engage with citizens and civil society for wider input and support;
- aspects of cybersecurity of the technology proposed, and the protection of communication systems and networks involved in the solutions, if and as relevant.

Proposals that include solutions and/or methods that would contribute to a lower environmental impact and footprint, better cost-efficiency, better energy-efficiency, and/or better operational autonomy of the capabilities and solutions in this topic, would be welcome.

Depending on the particular scope of the proposal, participation of Police Authorities, Border and/or Coast Guards is welcome.

In order to ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project’s mid-term outcomes, performed by the practitioners involved in the project. .

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

The provision of Financial Support to Third Parties is mandatory to give financial support to additional (i.e., beyond those partners in the Consortium) practitioners (i.e., authorities with competences of Customs) to engage during the project for additional piloting, testing and/or validation of technologies or methods. From 5% up to 20% of the EU funding requested by the proposal may be allocated to the purpose of financial support to third parties.

**Destination - Resilient Infrastructure**

As stated in the Horizon Europe Strategic Plan 2025-2027, proposals submitted under this Destination should aim to contribute to "*[…] resilience of large-scale interconnected systems' infrastructures and the bodies that operate them in case of complex attacks, pandemics, natural and human-made disasters, or the impacts of climate change[…]*". To this end, these proposals should contribute to the achievement of one or more of the following impacts:

- address both physical and digital aspects of critical infrastructure security, including specific challenges for cybersecurity, and
- support development of upgraded systems, and the interoperability of existing systems, for operators' resilience and the protection of critical infrastructure to enable a rapid, effective, safe and secure response and recovery, as also situational awareness and information sharing, without significant human involvement, to complex threats and challenges while also supporting emergency responders where their intervention is needed;
- security by design is a default feature of both newly created and upgraded infrastructures;
- improve cross-sectoral cooperation, as well as risk assessments to ensure the resilience and open strategic autonomy of European infrastructures.

More specifically, having in mind the fast pace of technological developments, growing dependencies of modern democratic societies, public administration and economies from critical infrastructure, as well as ongoing hybrid threats, and the impacts of climate change, diverse swiftly advancing challenges that European society faces merit dedicated research and innovation actions in the scope of this Destination. Some of these specific challenges are:

- mapping of critical infrastructure interdependencies leading to early threat identification and warning systems, mitigation plans and recovery procedures;
- supply chains of critical infrastructure;
- risk of unmanned platforms attacks on critical infrastructure;
- effective perimeter protection (e.g.: physical barriers, surveillance systems, access control, or cybersecurity measures) and monitoring including large area spanning infrastructure elements;
- new threats and hazards arising from climate change and/or the green transition, including widespread use of renewable energy sources;
- implementation of post-disaster recovery lessons to manage future exposure and vulnerability;

- lack of standards and advanced tools to conduct virtual and physical stress tests (sectoral and cross sectoral).

This destination will continue to support the policy objectives of the directives on the resilience of critical entities (CER Directive[31] and on network and information security (NIS2 Directive[32]. Further, submitted proposals should consider policy developments and meet some of the expectations stemming from the following EU legislation and policy documents, whichever would be relevant to the challenges addressed by the proposal:

- Security Union Strategy]COM (2020) 605 final.],
- EU Counter-Terrorism Agenda[33],
- EU Cybersecurity Strategy[34],
- NIS2 Directive[35],
- CER Directive[36],
- EU Adaptation Strategy[37],
- EU Maritime Security Strategy[38],
- Europe-wide Climate Risk assessment (EUCRA) and Commission Communication on Managing Climate Risks[39],
- Joint Framework on Countering Hybrid Threats[40] and the Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats[41];
- EU C-UAS Strategy[42] or
- EU Space Strategy for Security and Defence[43];
- EU Disaster Resilience Goals[44].

31 Directive (EU) 2022/2557.
32 Directive (EU) 2022/2555.
33 COM (2020) 795 final.
34 JOIN (2020) 18 final.
35 Directive (EU) 2022/2555.
36 Directive (EU) 2022/2557.
37 COM (2021) 82 final.
38 Council of the EU 11205/14.
39 COM (2024) 91 final.
40 JOIN (2016) 18 final.
41 JOIN (2018) 16 final.
42 COM (2023) 659 final.
43 JOIN (2023) 9 final.
44 (2023/C 56/01); COM (2023) 61 final.

Plans to build on elements of relevant predecessor projects should be considered, where relevant. It will be important also to take into account how research results can be advanced to deployable solutions after the projects lifetime, utilising validation and capacity-building programmes like the Internal Security Fund, or Digital Europe Programme.

Where possible and meaningful, synergy-building and clustering initiatives with successful actions in the same, or other relevant areas. should be considered, including the organisation of international events in coordination with the Community for European Research and Innovation for Security (CERIS).

Proposals are invited against the following topic(s):

**HORIZON-CL3-2025-01-INFRA-01: Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 15.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility conditions apply:<br>This topic requires involvement as beneficiaries of at least 3 relevant practitioners stemming from at least 3 different EU Member States or Associated Countries. Depending on the specific proposal submitted, these practitioners should represent one or several of the following portfolios: critical infrastructure operator, government authority responsible for critical infrastructure resilience, national authority responsible for overseeing critical infrastructure operators, or civil protection authority. For these participants, applicants must fill in the table “Information about security practitioners” in the application form with all requested information.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |

| | |
|---|---|
| *Technology Readiness Level* | ctivities are expected to achieve TRL 6-7 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Beneficiaries should provide financial support to third parties in the form of grants. The maximum amount to be granted to each third party is EUR 200 000 to support effective engagement with SMEs and/or effective collaboration and/or coordination with additional relevant critical infrastructure operator, government authority responsible for critical infrastructure resilience, national authority responsible for overseeing critical infrastructure operators, or civil protection authority from EU Member States or Associated Countries. These additional partners involvement should include testing and validation activities in the operational environment. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Critical infrastructure is more resilient to natural hazards, intentional and accidental harmful human actions, including cyberattacks;
- Critical infrastructure operators and authorities have better mapping of the interdependencies relevant for the addressed sector(s);
- Critical infrastructure operators and authorities have access to improved monitoring, risk and threat assessment, forecast, and if applicable modelling tools as well as cyber- and physical security solutions;
- Critical infrastructure operators and authorities have access to increased post-incident investigation capabilities contributing to better crisis prevention, preparedness, management and response;
- Effective digital tools to conduct virtual and physical stress tests are available for relevant security practitioners;
- Training curricula for critical infrastructure operators, authorities and/or first responders are developed.

Scope: Under this open topic, proposals are invited to address new challenges, and/or develop innovative solutions to existing challenges in order to increase the resilience of critical

infrastructure. Proposals should primarily address infrastructure sector(s) and/or interdependencies that are not covered, in particular by the past Horizon Europe calls: Resilient Infrastructure 2023 and Resilient Infrastructure 2024. If they relate to some of the topics covered by Horizon Europe Calls Resilient Infrastructure 2021-2022, the proposals should convincingly explain how they will build on and not duplicate them.

Adapted to the nature, scope and type of proposed activities, proposals should convincingly explain how they will plan and/or carry out demonstrations, testing or validation of developed tools and solutions. Proposals should also outline the plans to develop possible future uptake and upscaling at regional, national and/or EU level.

In order to ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment, performed by the practitioners involved in the project, of the project's mid-term outcomes.

In this topic, the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Proposals should plan their activities opting for the financial support to third parties in order to provide financial support to practitioners (critical infrastructure operator, government authority responsible for infrastructure resilience, national authority responsible for overseeing critical infrastructure operators, or civil protection authority) for expanding the proposed work in terms of additional user groups, complementary assessments, technology- or methodology-testing activities and/or to SMEs as additional solution providers in line with the conditions set out in Part B of the General Annexes. Consortium will define the selection process of the third parties for which financial support will be granted. From 10% up to 30% of the EU funding requested by the proposal may be allocated to the purpose of financial support to third parties.

Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication, exploit complementarities, and use opportunities for increased impact. Similarly, coordination with projects funded under HORIZON-CL3-2025-INFRA-01-02: Open topic for role of the human factor for resilience of European critical entities.

**HORIZON-CL3-2025-01-INFRA-02: Open topic for role of the human factor for the resilience of critical infrastructures**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |

| | |
|---|---|
| *Indicative budget* | The total indicative budget for the topic is EUR 7.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility conditions apply:<br>This topic requires involvement as beneficiaries of at least 3 relevant practitioners stemming from at least 3 different EU Member States or Associated Countries. Depending on the specific proposal submitted, these practitioners should represent one or several of the following portfolios: critical infrastructure operator, government authority responsible for infrastructure resilience, national authority responsible for overseeing critical infrastructure operators, or civil protection authority. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all requested information.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Critical infrastructure is more resilient to natural hazards, intentional and accidental harmful human actions, including cyber attacks;
- Infrastructure operators and authorities have better understanding of human factor for the critical entities resilience;
- Infrastructure operators and authorities have access to improved risk and threat assessment, and forecast;
- Infrastructure operators and authorities have access to increased post-incident investigation capabilities contributing to better crisis prevention;

- Effective digital tools to conduct virtual and physical stress tests are available for relevant security practitioners;
- Training curricula for infrastructure operators, authorities and/or first responders are developed.

Scope: Under this open topic, proposals are invited to address new challenges, and/or develop innovative solutions or strengthen capabilities to tackle existing challenges taking into account the human factor, including gender-related differences, for the benefit of resilience of critical infrastructures. The emphasis of the proposals should be on the abilities of critical infrastructure to cope with an adverse event, including their capacity to prepare for the crisis, absorb the impact, reduce the recovery time, and adapt by reducing future exposure and vulnerabilities.

In order to ensure the active involvement of, and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment, performed by the practitioners involved in the project, of the project's mid-term outcomes.

Activities proposed within this topic should address both technological and societal dimensions of the tackled challenge in a balanced way. This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of related research and innovation activities.

Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication, exploit complementarities, and use opportunities for increased impact. Similarly, coordination with projects funded under HORIZON-CL3-2025-INFRA-01-01: Open topic for improved preparedness for, response to and recovery from large-scale disruptions of European infrastructure.

**Destination - Increased Cybersecurity**

Proposals for topics under this Destination should set out a credible pathway contributing to the following impact of the Strategic Plan 2025-2027: "Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats".

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Support the EU's technological capabilities by investing in cybersecurity research and innovation to further strengthen its leadership, strategic autonomy, digital sovereignty and resilience;
- Help protect its infrastructures and improve its ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from cyber and hybrid incidents, especially given the current context of geopolitical change;
- Support European competitiveness in cybersecurity and European strategic autonomy, by protecting EU products and digital supply chains, as well as critical EU services and infrastructures (both physical and digital) to ensure their robustness and continuity in the face of severe disruptions;
- Encourage the development of the European Cybersecurity Competence Community, in close collaboration with the European Cybersecurity Competence Centre (ECCC) to avoid duplication;
- Particular attention will be given to SMEs, who play a crucial role in the cybersecurity ecosystem and in overall EU digital single market competitiveness, by promoting security and privacy 'by design' in existing and emerging technologies.

In accordance with Article 5(5) of Regulation (EU) 2021/88787, and subject to a contribution agreement as defined in point (18) of Article 2 of the Financial Regulation, the European Commission entrusts the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) with the implementation of the Increased Cybersecurity 2025 call (HORIZON-CL3-2025-CS-01). This entrustment may take place as soon as the ECCC has reached its financial and operational autonomy expected in the third quarter of 2024.

Proposals are invited against the following topic(s):

**HORIZON-CL3-2025-02-CS-01: Generative AI for Cybersecurity applications**

| **Call: HORIZON-CL3-2025-02 Civil Security for Society** |
|---|

| **Specific conditions** | |
|---|---|
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of between EUR 14.00 and 16.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 44.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries.<br>In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, may not participate in the action.<br>Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |
| *Procedure* | The procedure is described in General Annex F. The following exceptions apply:<br>To ensure a balanced portfolio covering a broad range of research areas, grants will be awarded to applications not only in order of ranking but at least also to the two highest ranked proposal addressing expected outcome a) and the highest ranked proposal addressing expected outcome b), provided that the applications attain all thresholds. |

Expected Outcome: Projects will develop technologies, tools, processes, that reinforce cybersecurity using AI technological components, in particular Generative AI, in line with relevant EU policy, legal and ethical requirements.

Proposals shall address at least to one of the following expected outcomes:

a. Developing, training and testing of Generative AI models for monitoring, detection, response and self-healing capabilities in digital processes, and systems against cyberattacks, including adversarial AI attacks.

b. Development of Generative AI tools and technologies for continuous monitoring, compliance and automated remediation. These should consider legal aspects of EU and national regulation as well as ethical and privacy aspects.

Scope: The use of Artificial intelligence is becoming indispensable with applications where massive data is involved. Understanding all implications for cybersecurity requires deeper analysis and further research and innovation.

Generative AI presents both opportunities and challenges in the field of cybersecurity. This topic supports the research on new opportunities brought by Generative AI for Cybersecurity applications, to develop, train and test AI models to scale up detection of threats and vulnerabilities, enhance response time, cope with the large quantities of data involved, and automate process and decision-making support; for example by generating reports from threat intelligence data, suggesting and writing detection rules, threat hunts, and queries for the Security information and event management (SIEM), creating management, audit and compliance reports and reverse engineering malware.

Proposals addressing expected outcome a)

(i) **Advanced threat and anomaly detection and analysis**: Current cybersecurity tools may struggle to keep pace with the evolving tactics of cyber attackers. Developing, training and testing of Generative AI models can be used to analyse large volumes of data and accurately identify anomalies and deviations from normal patterns of behaviour, enabling more effective threat detection, analysis and response.

Tools should also support cybersecurity professionals as they may struggle to detect and respond to threats posed by generative AI, particularly as these systems become more sophisticated and difficult to distinguish from genuine human activity.

(ii) **Adaptive security measures**: Cybersecurity tools often rely on static rules and signatures to detect threats, making them less effective against new and evolving attack methods. In addition, many cybersecurity tools still rely on manual intervention for threat response, which can be time-consuming and ineffective. Generative AI, through development, training, finetuning and testing of Generative AI models can support these tools to adapt and respond to emerging threats in real-time, improving overall security posture.

(iii) **Enhanced authentication and access control**: The use of AI technologies could improve authentication and access control systems to unauthorized access and credential theft, making it more difficult for unauthorized users to gain access to sensitive information or systems.

Proposals addressing expected outcome b)

(i) Development of tools powered by Generative AI that analyse and facilitate the **Application of the national and EU regulation in digital systems**, in particular the Artificial Intelligence Act, the Directive on measures for a high common level of cybersecurity across the Union (NIS2) and the Cyber Resilience Act.

(ii) **Adaptation to a dynamic environment**. Companies, public sector and organisations face an ever-changing environment which makes keeping up with compliance towards cybersecurity rules challenging. On one hand there's a variety of rules applicable at sectorial, national or European level to be considered. On the other, change management and updates in ICT systems in organisations is frequent. Addressing both facets with tools powered with Generative AI brings the potential for a compliance continuum within organisations otherwise limited in time when driven by human intervention only.

All proposals will have to respect Trustworthy and Responsible AI principles[45] and data privacy.

All proposals shall demonstrate the EU added value by fostering the development of EU technology, the use of open-source technologies when technically and economically feasible, the exploitation of available EU data (Data Spaces, EOSC, federated data etc)

Proposals must define key performance indicators (KPI), with baseline targets to measure progress should demonstrate how the proposed work will bring significant advancement to the state-of-the-art. All technologies and tools developed should be appropriately documented, to support take-up and replicability. Participation of SMEs is encouraged.

Proposals will pay special attention to the Intellectual Property dimension of the results. The usability of the outcomes and results once the project is finished will be closely assessed.

**HORIZON-CL3-2025-02-CS-02: New advanced tools and processes for Operational Cybersecurity**

| **Call: HORIZON-CL3-2025-02 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of between EUR 4.50 and 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 25.55 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this |

[45] https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/guidelines-responsible-use-generative-ai-research-developed-european-research-area-forum-2024-03-20_en
https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

| | |
|---|---|
| | topic is limited to legal entities established in Member States and Associated Countries.<br>In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, may not participate in the action.<br>Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |
| *Technology Readiness Level* | Tools and technologies developed are expected to start the project at minimum at TRL 4 and achieve at least TRL 7 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [46]. |

Expected Outcome: The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of the economy. Public administrations, companies and citizens are more interconnected and interdependent across sectors and borders than ever before. This higher uptake of digital technologies increases exposure to cyber security incidents and their potential impacts. At the same time, Member States are facing growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others.

Moreover, cyber operations are increasingly integrated in hybrid and warfare strategies, with significant effects on the target. In particular, the current geopolitical context is being accompanied by a strategy of hostile cyber operations, which is a game changer for the perception and assessment of the EU's collective cybersecurity crisis management preparedness and a call for urgent action. The threat of a possible large-scale incident causing significant disruption and damage to critical infrastructure and data spaces demands

[46] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

heightened preparedness at all levels of the EU's cybersecurity ecosystem. In recent years, the number of cyberattacks has increased dramatically, including supply chain attacks aiming at cyberespionage, ransomware, or disruption.

As regards detection of cyber threats and incidents, there is an urgent need to increase the exchange of information and improve our collective capacities in order to reduce drastically the time needed to detect cyber threats, before they can cause large-scale damage and costs. While many cybersecurity threats and incidents have a potential cross-border dimension, due to the interconnection of digital infrastructures, the sharing of relevant information among Member States remains limited. Proposals are expected to address this emerging threat landscape with the development of advanced frameworks, services tools, and processes, in line with relevant EU legislation (NIS2, Cyber Solidarity Act).

To develop innovative, frameworks, technologies, tools, processes, and services that reinforce cybersecurity capabilities for operational and technical cybersecurity cooperation, in line with relevant EU policy, with particular focus on NIS2, Cyber Solidarity Act and the EU Cybersecurity Strategy, as well as legal and ethical requirements.

Proposals shall address at least two of the following expected outcomes:

- Enhanced Situational Awareness through advanced Cyber Threat Intelligence frameworks, tools, and services as well as cybersecurity risk assessments of critical supply chains made in the EU,
- Frameworks, tools, and services for preparedness against Cyber and Hybrid Threats, including cybersecurity exercises,
- Expanded SOC/CSIRT functionality through advanced tools and services for Incident Handling, Reporting, Detection, Analysis and Response,
- Development of testing and experimentation facilities for advanced tools and processes for operational cybersecurity, including the creation of digital twins for critical infrastructures and essential and important entities as defined in NIS2,
- Development and pilot implementation of cross-sector and/or cross-border cyber crisis management frameworks, services, and tools,
- Frameworks, services, and tools targeting mechanisms and processes for enhanced operational cooperation between public sector entities (CSIRT network, EU-CyCLONe). Extension of the above to essential and important entities as defined in NIS2 would be an advantage.

Scope: Proposals are expected to demonstrate the developed frameworks, tools, services, and processes through pilot implementations with the participation of relevant national cybersecurity authorities and/or essential and important entities as defined in NIS2, implemented with the participation of leading European cybersecurity industry. Proposals shall consider the impact of forthcoming legislation, in particular the Cyber Resilience Act.

Real world applications and the usability of the solutions developed should feature predominately in the proposals.

Participation of innovative European cybersecurity start-ups and SMEs with a proven track-record in cybersecurity innovation at EU level (e.g. active participation in successful EU funded projects including cybersecurity projects under Horizon Europe, DEP cybersecurity projects or EIC Pathfinder or Accelerator projects, European start-ups and SMEs that can demonstrate established operational cooperation with relevant National Cybersecurity Authorities, European start-ups and SMEs that have received equity investments by national, European or private Venture Capital funds for cybersecurity activities etc. is highly encouraged. The participation of these start-ups and SMEs with an active role in the implementation of the proposed action (project coordination, technical coordination, lead of pilot implementation etc) would be considered an asset.

**HORIZON-CL3-2025-02-CS-03: Privacy Enhancing Technologies**

| **Call: HORIZON-CL3-2025-02 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of between EUR 3.00 and 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 11.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the |

| | |
|---|---|
| | Research and Training Programme of the European Atomic Energy Community (2021-2025). [47]. |

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Development of robust, scalable, and reliable technologies to uphold privacy and manage identities within federated and secure data sharing frameworks, as well as in the processing of personal and industrial data, integrated into real-world systems.
- Development of privacy preserving approaches for data sharing solutions, including privacy-preserving cyber threat information sharing, and in collaborative computations involving sensitive data.
- Integration of privacy-by-design at the core of software and protocol development processes, with attention to ensure that cryptographic building blocks and implementations of privacy-enhancing digital signatures and user-authentication schemes are crypto-agile and modular, to facilitate a transition towards post-quantum cryptographic algorithms.
- Development of privacy enhancing technologies for the users of constrained devices.
- Contribution towards the advancement of GDPR-compliant European data spaces for digital services and research, such as those on health data, aligning with DATA Topics of Horizon Europe Cluster 4.
- Development of privacy enhancing technologies and solutions, to benefit the requirements of citizens and companies, including small and medium-sized enterprises (SMEs).
- Development of blockchain-based and decentralized privacy-enhancing technologies, to preserve data confidentiality, integrity, and the authenticity of transactions and digital assets. Possible combination of blockchain with other technologies, such as federated learning, will need to address the data's security and privacy shared through such networks while ensuring that the networks' devices are trusted.
- Investigating the usability and user experience of privacy-enhancing technologies and exploring ways to design systems that are both secure and user-friendly.

Scope: Protecting individuals' personal data and ensuring privacy while allowing for data processing and analysis is fundamental for our society. Privacy-preserving techniques allow to minimize the amount of personal data collected and processed, and to protect that data

[47] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

through advanced cryptographic methods. For instance, machine-learning methodologies are leveraged to dissect medical and behavioural data, aiming to unearth causations and insights into cyber attacks or threats. However, a substantial portion of this data comprises personal information, (such as sensitive health data), raising concerns over potential breaches or misuse, thus jeopardizing the privacy of individuals, societal well-being, and economic stability.

In addition, the challenges related to the exploitation of non-personal/industrial data assets, which could impede the full realization of the data-driven economy, are also subject to the work that can be proposed under this topic. Solutions that can provide security against quantum adversaries are also encouraged.

Privacy-enhancing technologies (PETs) such as cryptographic anonymous credentials, differential privacy, secure multiparty computation, homomorphic encryption, advanced digital signatures, such as ring signatures, blind signatures and attribute-based credentials hold promise in mitigating these challenges, yet their practical application necessitates further refinement and rigorous testing. Consortia are encouraged to propose solutions that can improve the usability and effectiveness of different PETs in realistic environment and to investigate their integration within common European data spaces. The inclusion of agile schemes designed in a modular way to support the transition to post-quantum PETs and the design, improvement and security of quantum-resistant PETs is welcome, in light of the advances of quantum technologies.

Proposals should also focus on enhancing the usability, scalability, and dependability of secure and PETs within supply chains, while seamlessly integrating with existing infrastructures and conventional security protocols. They should also accommodate the diversity in data types and models across various organizations, undergoing validation and pilot runs within authentic data environments. Adherence to data regulations, notably GDPR, is paramount.

Consortia should seek to intertwine interdisciplinary expertise and resources from industry stakeholders, service providers, and end-users. The engagement of SMEs is encouraged, alongside the inclusion of legal proficiency to ensure regulatory compliance, including GDPR adherence. Furthermore, proactive identification and assessment of potential regulatory hurdles and constraints for the developed technologies/solutions are strongly encouraged.

**HORIZON-CL3-2025-02-CS-04: Security of Post-Quantum primitives**

| **Call: HORIZON-CL3-2025-02 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of between EUR 1.00 and 2.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |

| | |
|---|---|
| *Indicative budget* | The total indicative budget for the topic is EUR 4.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries.<br>In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, may not participate in the action.<br>Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [48]. |

Expected Outcome:

- Projects' results are expected to contribute to some or all of the following outcomes:
- breakthroughs in understanding the quantum hardness of various mathematical problem classes that underpin the security of current and future post-quantum cryptosystems;
- new quantum algorithms with significant quantum speed-up for lattice-based, code-based, and potentially other mathematical problem-classes;

[48] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- AI-based approaches to help discovering vulnerabilities of lattice-based or other mathematical problem-classes;
- cryptanalysis results;
- parameter suggestions to create a robust set of cryptographic building blocks for post-quantum cybersecurity and design of post-quantum cryptosystems with improved security against quantum or AI-based attacks.

Scope: The intrinsic security of PQC algorithms is based on mathematical problems that are believed to be intractable for both classical and quantum computers. To assess the quantum security of post-quantum primitives is fundamental in order to boost our confidence on post-quantum cryptosystems. The development of quantum algorithms demonstrating a significant quantum speed-up would represent a major breakthrough, necessitating a reassessment of the security of cryptosystems (lattice-based, code-based, and others). Conversely, if no significant quantum speed-up is discovered, it would bolster our confidence in the security of these post-quantum cryptosystems, though some parameters may still require fine-tuning. Studies are also needed on AI-based approaches that may be used to attack certain schemes with certain implementation choices, and the discovery of eventual vulnerabilities can help the research community develop more robust post-quantum cryptosystems.

Proposals on the assessment of the security of post-quantum primitives, via studies focused on eventual quantum algorithms with demonstrable speed-up, eventually also in combination with AI, or on solely AI-based approaches, are welcome. The security of lattice and code-based PQC algorithms may be prioritized, but tackling other mathematical problem classes is not excluded. As the unprecedented computational power of quantum computing can greatly enhance AI capabilities, combination of different approaches may also be considered. Consortia with team of applicants with background in post-quantum cryptography and in quantum computing are particularly encouraged. Project should lead to identification of vulnerabilities of current post-quantum cryptographic building blocks and to practical recommendations for parameters for the design of post-quantum cryptosystems with improved security against quantum attacks and future advances in code-breaking and AI.

**HORIZON-CL3-2025-02-CS-05: Security of implementations of Post-Quantum Cryptography algorithms**

| **Call: HORIZON-CL3-2025-02 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of between EUR 1.00 and 2.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 6.00 million. |

| | |
|---|---|
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries.<br>In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, may not participate in the action.<br>Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [49]. |

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Implementations of Post-Quantum Cryptography (PQC) algorithms that are resistant to side-channel and fault attacks;
- Optimized countermeasures taking into account a balanced trade-off between security, performance, and costs;
- Recommendations on implementing resilience for different types of attacks, also identifying the available and necessary hardware;

[49] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Analysis of new attacks or combinations of attacks, also eventually enhanced by AI, applicable to real-world conditions.

Scope: The security of the implementations of PQC algorithms is vital for maintaining the integrity, confidentiality, and availability of digital information and communications in the face of relevant side-channel, such as timing attacks, power monitoring attacks, and others, and fault attacks, etc. Such attacks, eventually also enhanced by the use of deep learning, constitute significant threats to both software-only and hardware implementations. In various application areas such as IoT, cloud-based applications, automotive, measures to preventing such attacks currently lead to substantial resource overhead due to the complexity of the algorithms and the limited exploration of different attack surfaces. In particular, countermeasures may have significant impact on run-time and memory consumption. Resistance in PQC implementations to side-channel and other relevant attacks is an increasingly common concern among customers, especially when exploring the right balance between security and performance.

Evaluating the resilience of PQC algorithm implementations against side-channel and fault attacks is crucial, given the proven vulnerabilities. Various countermeasures, such as masking, shuffling, randomized clocking, random delay insertion, constant weight encoding, code polymorphism, control-flow integrity and re-computation of critical operations can be employed to mitigate these attacks.

Proposals on implementations that protect against such attacks, at reasonable costs and minimizing the loss of performance while maintaining the required security, as well as on the analysis of new attacks or combinations of attacks, also powered by the use of AI, are welcome.

## Destination - Disaster-Resilient Society for Europe

Given the increasing frequency and ever greater impacts of disasters resulting from climate extremes, natural, geohazards and human-made hazards, the EU needs to invest more in improving disaster risk management, tools for first responders and societal resilience. In this respect, along the orientations given in the Horizon Europe Strategic Plan 2025-2027, the main objectives of this destination supporting the *reduction of losses from natural, accidental and human-made disasters* will be pursued in continuity with the strategic plan 2021-2024.

The Destination will support the implementation of UN Disaster Risk Reduction policies, the EU Disaster Resilience Goals[50], involving closer coordination with the Union Civil Protection Knowledge Network, the rescEU initiative and Member States' civil protection authorities, as well as an enhanced dialogue at international level with the United Nations Office for Disaster Risk Reduction (UNDRR) on recommendations for the Sendai Framework.[51]. Such closer coordination with other programmes will make it possible to further streamline future research programming. For example, Cluster 3 should focus on its core added value, which is a strong operational character for preparedness, response and learning, while maintaining complementarities with broader prevention issues such as climate-related risks, covered by Cluster 5, and the Mission on Climate Change Adaptation. There are similar examples in closer coordination with Cluster 6 and the One Health approach, regarding, for instance, water and food security threats (as a result of intentional degradation or terrorist acts).

From a technological perspective, the Destination will ensure greater involvement of practitioners in close cooperation with the Member States and EU agencies, not only in research development and implementation, but also the identification of gaps and needs and future research topics. Actions to develop tools and technologies to meet operational capability needs should be aimed at higher technological readiness levels (TRLs). Finally, it will be important to take into account how research results, both those still to come and those already developed in past projects under the DRS destination, can be turned into deployable solutions by being combined with capacity-building programmes (in particular the Internal Security Fund, funding under the Union Civil Protection Mechanism[52], the European Regional Development Fund, and the Cohesion Fund) and social innovation to support the entry into the market of developed technologies. Actions will also aim to ensure that there is a link between R&I and possible procurement (e.g., in the area of medical countermeasures).

Proposals for topics under this Destination should have the overarching objective of improving resilience. Actions will continue to explore initiatives and experiments involving the development of technological or methodological solutions for crisis management and support for emergency responders, getting the general public more involved in this area and improving interactions between regional and/or local authorities, public practitioners, private operators and civil society. Actions could also take into consideration regions vulnerable to

50 (2023/C 56/01); COM (2023) 61 final.

51 UNDRR, Sendai Framework for Disaster Risk Reduction 2015-2030

52 See the UCPM scientific needs assessment on disaster risk management: https://civil-protection-knowledge-network.europa.eu/media/outcome-report-scientific-research-needs-exercise.

extreme weather events in coastal areas, sea level rise and other climate change impacts, which may prone to disaster risks (e.g. the Arctic). New tools or solutions should build on what has been developed in past projects and be capable of being integrated into existing (legacy) systems. Actions will also focus on multi-service capability developments, in particular tools and technologies to support direct operational needs in case of a disaster. This will be done in a scalable way, covering areas from small rural towns to economically developed ones with a high population density, and opening research initiatives to international cooperation. Capabilities need to be upgraded to match the new resilience stakes and expectations of practitioners and of society as a whole. We should learn from past disaster events by identifying gaps in capabilities that the response to such events showed were lacking. For example, one of such gaps are the availability of medical countermeasures used to effectively respond to deliberate or accidental releases of CBRN substances.

The destination will continue to follow a multi-hazard approach, addressing disasters and threats of all kinds, including their cascading issues, climate-related or natural and geological hazards, industrial accidents, pandemics, intentional hostile acts including terrorism and armed conflict. Particular attention will be paid to floods and wildfires, as well as to chemical, biological, radiological, nuclear and explosive (CBRN-E) threats. To this end, proposals should contribute to the achievement of one or more of the following impacts:

- Enhanced citizen and regional and/or local authorities' involvement in research actions, and in operational measures that may result from research, with focus on risk awareness and enhanced disaster prevention and preparedness, including youth awareness raising and education;

- Improved disaster risk governance (from prevention, preparedness to mitigation, response, deployment of countermeasures and recovery, using updated risk assessment methods and decision criteria, and including knowledge transfer and awareness of innovative solutions) from international to regional and/or local levels;

- Strengthened capacities of first responders in all operational phases related to any kind of (natural and human-made, including hybrid threats) disasters in support of field operations with validation of tools and technologies used in disaster responses including emergencies, and demonstration of their interoperability.

More precisely, in the context of exacerbated impacts of various disaster threats on vulnerable societies, research and innovation actions are highly needed to face the many challenges faced by European Society. Some of them are:

- Challenges related to inclusion of the general public, regional and/or local communities and voluntary organisations as active partners in order to:

    - empower citizens to act and help them to improve their disaster risk awareness and own resilience to crises, including accountability for regional and/or local administrative decisions on residual risks, youth awareness raising and education;

  - provide means for regional and/or local decision-makers and operational responders, i.e., first and second responders, infrastructure owners, regional and/or local authorities (including public services, transport and utilities) to coordinate prevention and preparedness actions, bearing in mind the socio-economic and cultural context, and for operational responders to influence regional and/or local planning decisions that affect exposures and vulnerability to risks in short and long term;

  - address citizens' perception of, and involvement in, civil defence in the event of very large-scale disasters including armed conflict.

- Challenges regarding the reinforcement of disaster risk governance and the consideration of knowledge and innovative solutions in order to:

  - improve operational management of crises at different levels (prevention, preparedness, response, recovery) and scales (international to regional and/or local),

  - reinforce the uptake and transfer of knowledge to risk managers, first and second responders and decision-makers;

  - Strengthen resilience and enhancing protection strategies for emergency services and healthcare workers in case of disasters;

  - Enhance preparedness for optimised detection, prevention, response and control measures in case of bioterrorism or emerging diseases.

- Challenges related to the validation and usability of tools and technologies, including the demonstration of their interoperability, in the context of strengthened first responder's capacities as to:

  - enhance risk awareness, preparedness and communication about foreseeable impacts of disasters;

  - deploy innovative solutions in emergency situations including trusted communication channels, medical care, medical countermeasures, support equipment (e.g. detectors), triage of victims as well as protection of first responders;

  - enhance validation of tools, technologies and processes for cross-border prevention, decision-support and responses to climate-related and geological disasters and emergency crises by different practitioner sectors (firefighters, medical emergency services, civil protection, police, NGOs);

  - enhance interoperability of tools and technologies used in international emergency (real-case) situations related to natural hazards, CBRN threats and hybrid threats

via inputs such as standard operating procedures for foresight, risk analysis or guidance with the aim to improve market uptake.

This Destination will also support, whenever appropriate and applicable, the proposals with some or all of the following goals:

- a clear strategy from international to regional and/or local on how the overall society will adapt to the evolving disaster risks based on the subsidiarity principle (from the citizen level to international decision-making);
- the involvement of different responders (firefighters, civil protection, medical emergency, police) and regional and/or local authorities in research, development and validation of methods and tools;
- the active role for Non-Governmental Organisations (NGOs) and Civil Society Organisations (CSOs);
- the active involvement of Small and Medium Enterprises (SMEs);
- a robust plan on how they will build on the relevant predecessor projects, and clustering with existing research (EU and national) actions to maximise complementarities and synergies and avoid duplication of efforts;
- education and training aspects for first and second responders for different types of threats (climate-related, geohazards, accidental, intentional), as well as information sharing and awareness raising of the citizens;
- a clear strategy on the uptake of the outcomes, defined in consultation with the involved stakeholders;
- a well-developed plan both on how research data for training and testing will be obtained, in order to reach the requested Technology Readiness Levels (TRLs), and on how the specific TRL will be measured.

Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, including the organisation of international conferences in close coordination with the Community for European Research and Innovation for Security (CERIS) activities and/or other international events.

Proposals are invited against the following topic(s):

**HORIZON-CL3-2025-01-DRS-01: Open topic on citizen and regional and/or local authorities' engagement in enhanced disaster risk awareness, including education, and preparedness**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** |
|---|
| **Specific conditions** |

| | |
|---|---|
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 12.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility conditions apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Regional and/or Local Authorities, at least 2 organisations representing citizens or regional and/or local communities[53] and 2 First Responders from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one project that is the highest ranked within each of the two options given in the scope (Option a and Option b), provided that the applications attain all thresholds.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [54]. |

[53] A Citizen Organisation can be a Non-Governmental Organisation representing citizens interests in the area of civil protection and/or associations of volunteers.

[54] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:

Expected Outcome: Project results are expected to contribute to one or both of the following expected outcomes:

- Improved disaster preparedness, learning from past disasters or crises, and better sharing of knowledge on lessons learned and risk awareness to citizens and regional and/or local authorities, understanding what countermeasures were taken in previous incidents and exploring currently available products to improve future outcomes;

- Reinforced dialogue and cooperation among scientific and technical communities, stakeholders, policy-makers and regional and/or local communities in disaster risk reduction for an enhanced uptake of research outputs.

Scope: Societal resilience and preparedness to disasters are shaped by the way authorities and citizens exchange, access, understand, and react to information about hazards. As a result, anyone may become more vulnerable if barriers to these processes occur. Strengthening societal resilience to disasters, therefore, requires investment by authorities at operational, strategic, and policy levels to improve engagement with citizens and integrate inclusive communication processes. In order to achieve this, it is important to take into account the diversity of citizens, be it relating to age, gender, educational levels, disability, and other social characteristics.

Under the Open Topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions and technology, including the use of AI, for improving disaster preparedness, risk awareness by citizens and regional and/or local authorities, and for reinforcing the cooperation among scientific / technical communities and policy-makers / regional and/or local authorities for an enhanced sharing of knowledge and uptake of research outputs. If they relate to some of the topics covered by Horizon Europe Calls Disaster-Resilient Society 2021-2022 or 2023-2024, the proposals should convincingly explain how they will build on and not duplicate them.

Proposals are expected to address one of the following options:

**Option a**: Tools and solutions to improve disaster preparedness and risk awareness by citizens and regional and/or local authorities;

**Option b**: Mechanism to enhance dialogue among research/academic communities, practitioners and regional and/or local authorities for sharing knowledge and effectively uptake research results.

Adapted to the nature, scope and type of proposed projects, proposals should convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Furthermore, proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is

---

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

finalised. Proposals should also consider, build on if appropriate and not duplicate previous research, including but not limited to research by other Framework Programmes' projects. Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

Proposals funded under this topic are expected to engage with citizen organisations, regional and/or local authorities and practitioners (first and second responders), private sector operators during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the Disaster Risk Reduction community.

This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of related research and innovation activities.

**HORIZON-CL3-2025-01-DRS-02: Open topic on Improving disaster risk management and governance to ensure self-sufficiency and sustainability of operations in support of enhanced resilience**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 10.50 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Due to the scope of this topic, legal entities established in all member states of LAC (Latin America/African/Caribbean) as well as Central Asian Countries are exceptionally eligible for Union funding.<br>Whereas legal entities established in low- and middle-income countries from the LAC (Latin America and Caribbean), African, and Central Asian are automatically eligible for funding, legal entities established in high-income countries from those regions are exceptionally eligible for Union funding under this topic.<br>The following additional eligibility conditions apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 |

| | |
|---|---|
| | Regional and/or Local Authorities, 1 Emergency Responder and 1 Volunteers Organisation from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br><br>To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one project that is the highest ranked within each of the two options given in the scope (Option a and Option b), provided that the applications attain all thresholds.<br><br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [55]. |

Expected Outcome: Project results are expected to contribute to the following expected outcome(s):

- Better understanding of the impact of disasters and crises, and improved early warnings and long-term planning linked to natural causes or to human-made threats (including CBRN) on risk governance, including emergency services, regional and/or local authorities, and citizen volunteers, and improved adaptation and resilience of emergency systems for disaster prevention and preparedness – especially in a multi-risk environment with cascading disasters.

Scope: Improved risk governance, adaptation and resilience requires authorities and communities to adopt risk and resilience management approaches, which are inclusive (including regarding gender, age, disabilities, etc.) and innovative, through pre-defined plans and procedures, as well as through adaptable and flexible capabilities to prepare for, respond to, recover from and learn from disasters and crises. It requires the implementation of policies

[55] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

at different levels (international to regional and/or local) and strategies for a better understanding of impacts and enhanced risk preparedness and adaptation, which are co-developed and enabled through *all-of-society* engagement and participation, and hence strengthen resilience to disasters among authorities, decision-makers, private actors, intermediary actors, volunteers and citizens, and the most vulnerable.

Under the Open Topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for an enhanced understanding of impacts of disasters and crises linked to natural or human-made causes on risk governance and improved resilience of emergency systems, that are not covered by topics of Horizon Europe Calls Disaster-Resilient Society 2023-2024. If they related to some of the topics covered by Horizon Europe Calls Disaster-Resilient Society 2021-2022, the proposals should convincingly explain how they will build on and not duplicate them.

Proposals are expected to address one of the following options:

**Option a**: Enhanced impact forecasting and early warning systems, understanding of climate / weather extreme events and geohazards and adaptation of emergency systems for disaster prevention and preparedness;

**Option b**: Enhanced impact forecasting and understanding of Chemical, Biological, Radiological, Nuclear, Explosive (CBRN-E) threats and adaptation of emergency systems for disaster prevention preparedness and response (including medical countermeasures). Projects need not address all elements of CBRN-E.

Adapted to the nature, scope and type of proposed projects, proposals should also convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Furthermore, proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on if appropriate and not duplicate previous research, including but not limited to research by other Framework Programmes' projects. Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

Proposals funded under this topic are expected to engage beyond the project consortium with volunteers' organisations, regional and/or local authorities and emergency services (first and second responders) during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the Disaster Risk Reduction community.

In order to ensure the active involvement of and timely feedback from relevant practitioners, i.e., emergency responders (with expertise in the different types of natural or human-made threats), proposals should plan a mid-term deliverable consisting in the assessment, performed by the practitioners involved in the project, of the project's mid-term outcomes.

This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of related research and innovation activities.

**HORIZON-CL3-2025-01-DRS-03: Open topic on Testing / validating tools, technologies and data used in cross-border prevention, preparedness and responses to climate extreme and geological events and chemical, biological or radiological emergency threats**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 13.50 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Due to the scope of this topic, legal entities established in all member states of LAC (Latin America/African/Caribbean) as well as Central Asian Countries are exceptionally eligible for Union funding.<br>Whereas legal entities established in low- and middle-income countries from the LAC (Latin America and Caribbean), African, and Central Asian are automatically eligible for funding, legal entities established in high-income countries from those regions are exceptionally eligible for Union funding under this topic.<br>The following additional eligibility conditions apply:<br>For each of the three options, this topic requires the active involvement, as beneficiaries, of at least 2 First Responders, and 2 SMEs from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table “Information about security practitioners” in the application form with all the requested information, following the template provided in the submission IT tool.<br>To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one project that is the highest ranked within each of the three options (Option a, Option b and Option c), provided that the applications attain all thresholds. |

| | |
|---|---|
| | If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL of 7-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [56].<br>Beneficiaries should provide financial support to third parties in the form of grants. The maximum amount to be granted to each third party is EUR 100 000 to support effective collaboration and/or coordination with relevant First Responders covering different disciplines and sectors of intervention, including testing and validation activities within the projects, and/or SMEs from EU Member States or Associated Countries. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to the following expected outcome(s):

- Enhanced European and global interoperability of existing tools and technologies and improved capacities to prevent, better prepare and respond to different types of disasters (natural and human-made) by various practitioners (e.g., firefighters, medical responders, civil protection).

Scope: The use of artificial intelligence (AI) and machine-learning (ML) tools is increasingly at the core of first responder's decision-making processes, including situational awareness, analysis and planning. Besides the needs to develop AI and ML tools, ground technologies such as miniaturised sensors that can operate autonomously for a long period in harsh

[56] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

environments and are fast and easy to deploy are needed for threat detection (such as chemical, biological or radiological substances) and/or identification of victims and possible locations for intervention. In addition, responders need to exchange information (language, data, video, etc.) in a reliable, secure, and universal way, while emergency communications throughout the European Union also need to be strengthened [57]. In many instances, interoperability of tools, technologies and communication channels is still an open issue, requiring standard operating procedures, specific education, training and exercises of responders.

Under the Open Topic, proposals are welcome to testing / validate tools, technologies and data used in cross-border prevention, preparedness and responses to climate / geological / accidental fire disasters and chemical, biological or radiological emergency threats (including medical countermeasures) by different practitioner's sectors in view of demonstrating their interoperability in real-case situations, with focus on the use of AI and ML tools, miniaturized sensors for threat detection and victim identification, and communication (including cross-border emergency communications).

Proposals are expected to address one of the following options focused on testing / validation of tools and technologies, and demonstration of their interoperability:

**Option a**: Use of artificial intelligence (AI) / machine learning (ML) tools to support first responder's analysis, planning and decision-making;

**Option b**: Miniaturized sensors for threat detection and victim identification;

**Option c**: Information exchange / Communication among first responders in a reliable, secure and universal way, and cross-border emergency communications;

**Option d:** Alert system to detect chemical threats, integrating different systems at national, regional and European levels.

Adapted to the nature, scope and type of proposed projects, proposals should also convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Furthermore, proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on if appropriate and not duplicate previous research, including but not limited to research by other Framework Programmes' projects. Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

Proposals funded under this topic are expected to engage beyond the project consortium with First Responders, Industry/SMEs and Standardisation Organisations during the lifetime of the

[57] Critical Communication System (EUCCS). See e.g., Commission White Paper on "How to master Europe's digital infrastructure needs?" (2024).

project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the Disaster Risk Reduction community.

In order to ensure the active involvement of and timely feedback from relevant practitioners, i.e., First Responders with expertise in the different types of natural or human-made threats, proposals should plan a mid-term deliverable consisting in the assessment, performed by the practitioners involved in the project, of the project's mid-term outcomes.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Proposals that include solutions and/or methods that would contribute to a lower environmental impact and footprint, better cost-efficiency, better energy-efficiency, and/or better operational autonomy of the capabilities and solutions in this topic, would be welcome.

Proposals should plan their activities opting for the Financial Support to Third Parties in order to provide financial support to practitioners (First Responders covering different disciplines and sectors of intervention) for expanding the proposed work in terms of additional user groups, complementary assessments, technology- or methodology-testing activities and/or to SMEs as additional solution providers in line with the conditions set out in Part B of the General Annexes. Each consortium will define the selection process of the third parties for which financial support will be granted. From 5% up to 20% of the EU funding requested by the proposal may be allocated to the purpose of financial support to third parties.

This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of related research and innovation activities.

**Destination - Strengthened Security Research and Innovation**

Since the Preparatory Action for Security Research[58], the EU-funded security research and innovation programme has contributed substantially to knowledge and value creation in the field of internal security. The programme has been fundamental to the consolidation of a European security ecosystem, which is better equipped to capitalise on research and innovation outcomes to support the EU security priorities. This Destination aims to contribute to reducing thematic fragmentation, bringing closer together the actors from different security domains, and expanding the market beyond traditional thematic silos. It also creates knowledge and value through research in matters (including technology, but also social sciences and humanities) that are not exclusive of only one security area, but cross-cutting to the whole Cluster.

As underlined in the Horizon Europe Strategic Plan 2025-2027, proposals for the topics under this Destination '*should support with cross-cutting actions the expected impacts outlined above [in the Cluster 3 Destinations]. The destination will increase the impact of the work carried out in the EU security Research and Innovation (R&I) ecosystem and contribute to its core values, namely:*

- *a focus on the potential final use of the outcomes of security R&I;*
- *forward-looking planning of EU security capabilities;*
- *the development of security technologies that are socially acceptable, developed in quadruple helix*[59]*, and that have added value for industrialisation, joint procurement, commercialisation, and the acquisition and deployment of successful R&I outcomes;*
- *safeguarding the EU's open strategic autonomy and technological sovereignty in critical security areas by contributing to a more competitive and resilient EU civil security technology and industrial base;*
- *experimenting with research and innovation programming; and*
- *helping to make the European R&I ecosystem more consistent'.*

Many of the programme outcomes have materialised in relevant scientific findings, maturation of promising technology areas, operational validation of innovative concepts or support to policy implementation. However, a key challenge remains in improving innovation uptake and thus contributing to the development of security capabilities[60], support of Start-ups

58 COM(2004) 72.

59 through the interaction of public authorities, academia, industry and the public.

60 For the purpose of the work programme, the terms "Capability" should be understood as "the ability to pursue a particular policy priority or achieve a desired operational effect". The term "capability" is often interchanged with the term "capacity", but this should be avoided. "Capacity" could refer to an amount or volume of which one organisation could have enough or not. On the other hand, "capability" refers to an ability, an aptitude or a process that can be developed or improved in consonance with the ultimate objective of the organisation.

and Small-Medium Enterprises (SMEs) and deployment of innovation by security practitioners.

The extent to which innovative technologies developed thanks to EU R&I investment are industrialised and commercialised by EU industry, and acquired and deployed by end-users, could reflect the impact achieved with the programme. As explained in the Commission staff working document on Enhancing security through research and innovation[61], there are factors inherent to the EU security ecosystem (often attributed to the market) that hinder the full achievement of this impact, such as market fragmentation, cultural barriers, analytical weaknesses, programming weaknesses, ethical, legal and societal considerations or lack of synergies between funding instruments, among others. To that aim, there is a need to create a favourable environment that is designed with the main purpose of increasing the impact of security R&I, which provides the right tools that serve to tackle the factors that hinder innovation uptake.

Therefore, security research and innovation shall foster and enhance the development of innovative tools, technologies and capabilities for the benefit of practitioners that can use in their day-to-day work. To this end proposals under this Destination should set out a credible pathway to contributing to the following impacts:

- A more effective and efficient evidence and knowledge-based development of EU civil security capabilities built on a stronger, more systematic and analysis-intensive security research and innovation cycle;
- Increased cooperation between demand and supply market actors, including with actors from other domains, fosters swift industrialisation, commercialisation, adoption and deployment of successful outcomes of security research and reinforces the competitiveness and resilience of EU security technology and industrial base and safeguards the security of supply of EU-products in critical security areas;
- R&I-enabled knowledge and value in cross-cutting matters reduces sector specific bias and breaks thematic silos that impede the proliferation of common security solutions.

The Destination will trigger actions that will help bringing these and other developments closer to the market, thus contributing to the measures facilitating the uptake of innovation. Those actions will help developers (including industry, research organisations and academia) to accelerate product development and improve the valorisation of their research investment. They will also support buyers and users in materialising the uptake of innovation and further develop their security capabilities. The aim is to increase the capacity of EU public procurers to align their requirements with the EU security industrial capacity and to attract innovation and innovators from security and other sectors through common validation strategies, rapid innovation, experimentation and pre-commercial procurement.

[61] https://home-affairs.ec.europa.eu/document/download/ff888398-0b0a-4511-9717-ad41beb22314_en?filename=SWD-2021-422_en.PDF

Finally, the Destination will contribute to the development of the tailored analytical capacity required for the adoption of capability-driven approaches aimed at fostering a forward-looking capability-driven approach in security.

Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, including the organisation of international conferences in close coordination with the Community for European Research and Innovation for Security (CERIS)[62] activities and/or other international events.

Proposals are invited against the following topic(s):

**HORIZON-CL3-2025-01-SSRI-01: National Contact Points (NCPs) in the field of security and cybersecurity fostering the links with National Community building for Safe, Secure and Resilient Societies**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 3.00 million. |
| *Type of Action* | Coordination and Support Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility conditions apply:<br>Applicants must be Horizon Europe national support structures (National Contact Points - NCPs),<br>NCP) responsible for Cluster 3 and officially nominated to the European Commission from an EU Member State or an Associated Country. |
| *Procedure* | The procedure is described in General Annex F. The following exceptions apply:<br>The granting authority can fund a maximum of one project. |

Expected Outcome: Project results are expected to contribute to some or all of the following outcomes:

[62] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

- Improved and professionalised NCP[63] service of knowledge, experience and skills, consistent across Europe, thereby helping simplify access to Horizon Europe calls, lowering the entry barriers for newcomers, and raising the average quality of proposals submitted;

- Harmonised and improved trans-national cooperation between NCPs, and support of National communities for research and innovation in the area of security that can collect input from practitioners, industrial partners and convey capability needs.; Increased cooperation of NCPs with seamless collaboration of the national initiatives, with the EU initiatives, namely CERIS[64];

- Periodic and timely evidence-based feedback in support to EU-funded security research programming enabled by a seamless integration of the national, regional and local dimensions of security Research and Innovation into the EU picture;

- A systematic assessment of the needs of the various stakeholders involved in the areas of security and increase the visibility of capability needs, gaps, and technology solutions expressed by national, regional and local communities;

- Improvement of the awareness of EU funding opportunities relevant for civil security research and innovation;

- Improvement of the awareness of innovation-uptake success stories stemming from the participation of national players in EU-funded security research projects;

- Reduced geographical fragmentation of the civil security research and innovation community via the cooperation with the various initiatives of National Communities of security research and innovation with the participation of stakeholders from the security ecosystem, that are set up and running in the different Member States or Associated Countries.

Scope: National Contact Points (NCPs) are support structures that have become an essential component in the implementation of successive Framework Programmes. They provide information and on-the ground advice to potential applicants and beneficiaries, through the project life cycle, in their own language, in a manner that would be impossible for the European Commission and its Agencies acting alone.

NCPs can benefit in their work from the sharing of best practices among them. NCPs can also help to give visibility to different perspectives of all Security Research and Innovation (R&I) stakeholders and to break geographical silos by aggregating the knowledge existing in the EU Member States and regions and incorporate it to the European picture. This set-up increases the visibility of the security at EU level and across security areas.

63 Link for Horizon Europe NCP model.
64 Link for Horizon Europe NCP model.

However, the security sector exhibits a remarkable geographic fragmentation, with actors operating at EU level, at national level, at regional level and even at local level. In order to acknowledge the different perspectives of all stakeholders and break geographical silos, there is a need to aggregate the knowledge existing in the Member States and Associated countries and incorporate it to the European picture.

Cooperation with national stakeholders and establishment of stronger links with the Community for European Research and Innovation for Security (CERIS)[65].

These links shall help to have a more comprehensive view of the common EU security needs and solutions, to better capitalise on pan-European cooperation and funding opportunities, and to give visibility to results from EU and other research projects.

Proposals shall link NCPs with national communities for research and innovation that exist already or will be established. The idea of this link is to identify capability gaps, solutions to address those gaps, and research needs at local, regional and national level and integrate them in the EU picture in collaboration with CERIS.

In addition, this collaboration will assist NCPs to share research opportunities coming from national research programmes and initiatives with the wider security research community at national level. This will also improve the visibility of the results achieved by national players following their participation in research projects (national or EU-funded), and in particular those which have led to the deployment of solutions in the field of operations, or which have a strong potential for uptake as a result of the interest expressed by national buyers.

Finally, this will support the promotion of innovation uptake with financial pathways and opportunities to enable the uptake of innovative solutions stemming from EU, national or regional capacity building funds, with special emphasis on the EU Home Affairs funds (both in the parts under shared management and those under direct management by the Commission) and on the European Regional Development Funds.

As an output of the action, the beneficiaries shall develop a model for the cooperation and enlargement of with the national research and innovation communities beyond the lifetime of the project and independent of EU security research funding. The objective is to support the establishment of self-standing national communities beyond the duration of the project.

The successful proposal will contribute to delivering the Programme’s objectives and impacts and raise awareness of potential applicants for calls under Horizon Europe Cluster 3 – "Civil Security for Society". Irrespectively of their sector or discipline, project proposals should aim to facilitate trans-national co-operation between NCPs, with a view to identifying and sharing good practices and raising the general standard of support to Programme applicants. The project should also allow for a better flow of information relevant for the implementation of the Programme from the EU level to the national level and vice-versa, and also across

[65] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

Member States and Associated Countries. This includes fostering the participation of national players in EU security research and innovation fora. Particular attention should be given to results that have led to the deployment of solutions in the field of operations, or that show a strong potential for uptake because of the interest expressed by national buyers.

Proposals should link up potential participants from widening countries with emerging consortia in the domain of the Cluster "Civil Security for Society" building on previous initiatives from similar past projects. Matchmaking should take place by means of online tools, brokerage events, info days and bilateral meetings between project initiators and candidate participants from widening countries. Other matchmaking instruments may be used as appropriate. The project proposal to be funded should cover a wide range of activities related to Horizon Europe, address issues specific to the Cluster "Civil Security for Society" and may follow up on the work of SEREN5.

Network to organise matchmaking activities in accordance with Annex IV of the NCP Minimum Standards and Guiding Principles. Proposals should also take into account support activities for coordination between the respective beneficiary (NCP) and the respective National Coordination Centre[66] within the relevant Member States as applicable once the regulation mentioned above is in force.

The project consortium should have a good representation of experienced and less experienced NCPs.

The recommended duration of the project is 3 years.

**HORIZON-CL3-2025-01-SSRI-02: Uptake Acceleration Services**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 5.00 million. |
| *Type of Action* | Coordination and Support Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility conditions apply: |

[66] National Coordination Centres according to regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.

| | |
|---|---|
| | Participation as beneficiaries of at least 2 Research and Technology Organisations is required. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The rules are described in General Annex G. |

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- To offer advanced services on innovation uptake to the security community;
- To provide a self-sustained mechanism for advanced advisory and support services, to act as a market catalyst; and to accelerate the uptake of innovation for security;
- Enhanced cooperation between research institutions, smaller private research agencies, security practitioners, Start-ups and SMEs to support innovation uptake;
- Strengthening the technology transfer from research to the market and strengthening of security ecosystem. Supporting Start-ups and SME to reach the security market and strengthen the capacity of security practitioners to uptake innovative tools from the security market.

Scope: The uptake of innovation stemming from EU-funded security research is not a single-step process, and there is no single method of ensuring the market uptake of successful research results. Innovation uptake needs to be contemplated as a long process that is conditioned by a number of enabling actions to be taken before research is even planned and long after it is completed. However, market uptake and deployment of innovation by security practitioners are recurrent challenges in civil security research.

The EU-funded security research ecosystem has changed the traditional relationship between practitioners and solution providers. The awareness of security needs and solutions has been steadily growing at all levels during the last years, with EU funded security research and innovation projects playing a pivotal role. This awareness guarantees not only that research addresses critical needs, but also that the research investment will deliver tangible results.

There are several approaches to achieve a better market uptake and to ensure that innovation can pass from the realm of research to the realm of the market and eventually innovative tools to be used by security practitioners.

In order to support SMEs and start-ups but also practitioners to find the avenues of uptake of innovation, models and methods for transferring research to the market should be promoted. This topic aims to offer services and guidance to entities in the security ecosystem to achieve market uptake.

The services should be delivered to SMEs/Start-ups and Practitioners. Therefore, there would be Supply-oriented Services and Demand-oriented services.

Some of the expected services could be open for the whole community (e.g., material online) whereas others would be provided upon specific request by an entity (on demand services). On demand services may be linked to other EU-funded actions but should not cover activities already funded from those in order to avoid double funding.

Applicants should be able to demonstrate a proven experience in technology development and innovation in the area of security and deep knowledge on the security ecosystem.

Successful candidates should be able to provide services such as:

- Funding & procurement guidance
- Market research / competitive landscaping / Marketplaces / Market surveys/consultations
- Proof of concept development (for TRL 2-4)
- Funding and tendering observatory
- Investor search / venture building
- Technology validation support Lab testing support (i.e., Readiness assessment, Artificial Intelligence act compliance, Machine Learning security, Ethical Legal and Societal assessment, High Performance Computing capabilities, Synthetic data generation, Access to Datasets, stress testing etc.)
- Tech and/or entrepreneurial skills development (training)

The proposals should outline the methods and processes by which they intend to decide which organisations they provide support to, respecting principles such as transparency, equal treatment, non-discrimination between organisations and effectiveness (impact). The project should provide suggestions for such methods and processes as deliverable to be approved by the European Commission. The applicants submitting the proposals have to ensure sufficient representativeness of the communities of interest (including, but not only, geographical representativeness) and a balanced coverage in terms of knowledge and skills of the different knowledge domains required to face the challenge, including security operations, technologies, research & innovation, industry, market, etc. The applying consortia need to demonstrate that the project beneficiaries guarantee the expertise required to steer the project activities in all the knowledge domains to ensure the success of the action. The work of the partners has to be supported by solid and recognised tools and methods, also accompanied by the required expertise to put them in practice.

Proposals should take into account the work initiated by the Networks of Practitioners funded under H2020 Secure Societies work programmes and the ongoing work of Knowledge

Networks. Proposals should build to the extent possible on the outcomes of previous initiatives that foster innovation uptake (e.g., iProcureNet[67], Multirate[68], etc). In addition, existing initiatives like Horizon Booster[69], EACTDA[70] and EAFIP[71] have some components which could be used by the successful project and to be adapted in the area of security.

The project has to identify and describe options for the sustainability of the services beyond the project lifetime, including the setting up of a permanent scheme which will continue to offer the proposed services to the community as a self-sustainable mechanism.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

The project should have a maximum estimated duration of 5 years.

The provision of financial support to third parties in the form of grants is optional.

**HORIZON-CL3-2025-01-SSRI-03: Open grounds for pre-commercial procurement of innovative security technologies**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 1.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 2.00 million. |
| *Type of Action* | Coordination and Support Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility conditions apply:<br>This topic requires the participation, as beneficiaries, of at least 6 end-user organisations as well as at least 3 public procurers. These beneficiaries must be from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table “Information about security practitioners” in the application form |

67 https://www.iprocurenet.eu/
68 https://www.multirate.eu/
69 https://www.horizonresultsbooster.eu/
70 https://www.eactda.eu/
71 https://eafip.eu/

| | |
|---|---|
| | with all the requested information, following the template provided in the submission IT tool.<br><br>One organisation can have the role of end-user and public procurer simultaneously, both counting for the overall number of organisations required for eligibility.<br><br>Open market consultations carried out during this project must take place in at least three EU Member States or Associated Countries. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [72]. |

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Consolidated demand for innovative security technologies built on the aggregation of public buyers with a common need expressed in functional and/or operational terms without prescribing technical solutions;
- Better informed decision-making related to investment in innovative security technologies based on a better understanding of the potential EU-based supply of technical alternatives that could address common needs of EU public buyers;
- Better informed decision-making related to investment in innovative security technologies based on an improved visibility of the potential demand in the EU market for common security technologies;
- Increased capacity of EU public procurers to align requirements with industry and future products and to attract innovation and innovators from security and other sectors through common validation strategies, rapid innovation, experimentation and pre-commercial procurement;

[72] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Increased innovation capacity of EU public procurers through the availability of innovative tendering guidance, commonly agreed validation strategies and evidence-based prospects of further joint procurement of common security solutions.

Scope: End-users and public procurers from several countries are invited to submit proposals for a preparatory action that should build the grounds for a future Pre-Commercial Procurement (PCP) action. Both this preparatory action and the future PCP action are open to proposals oriented to the acquisition of Research and Development (R&D) services for the development of innovative technologies, systems, tools or techniques to enhance border security, to fight against crime and terrorism, to protect infrastructure and public spaces, and/or to make societies more resilient against natural or human-made disasters.

In preparing the grounds for a possible future PCP action, the outputs of this Coordination and Support Action (CSA) should take into consideration:

- The policy priorities described in this Work Programme Part for the security areas mentioned above;
- The EU Directive for public procurement and in particular with the provisions related to PCP;
- The specific provisions and funding rates of PCP actions and the specific requirements for innovation procurement (PCP/PPI) supported by Horizon Europe grants, as stated in the General Annex H of the Horizon Europe Work Programme;
- The guidance for attracting innovators and innovation, as explained in the European Commission Guidance on Innovation Procurement C(2021) 4320, in particular those measures oriented to reduce the barriers to high-tech start-ups and innovative SMEs.

During the course of the project, the applicants are expected to deliver clear evidence on a number of aspects in order to justify and de-risk a possible follow-up PCP action, including:

- That the challenge is pertinent and that indeed a PCP action is required to complete the maturation cycle of certain technologies and to compare different alternatives;
- That there is a consolidated group of potential buyers with common needs and requirements which are committed to carry out a PCP action in order to be able to take an informed decision on a future joint procurement of innovative solutions;
- That there is a quantifiable and identifiable community of potential buyers (including and beyond those proposed as beneficiaries in the proposal) who would share to a wide extent the common needs and requirements defined and who could be interested in exploring further joint-uptake of solutions similar to those developed under the PCP, should these prove to be technologically mature and operationally relevant by the end of the project;

- That the state of the art and the market (including research) has been explored and mapped, and that there are different technical alternatives to address the proposed challenge;
- That a future PCP tendering process is clear, that a draft planning has been proposed and that the supporting documentation and administrative procedures will be ready on due time in order to launch the call for the acquisition of R&D services according to the PCP rules;
- That the technology developments to be conducted in the future PCP can be done in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data;
- That in developing technology solutions, societal aspects (e.g., perception of security, possible side effects of technological solutions, societal resilience) can be taken into account in a comprehensive and thorough manner.

If the applicants intend to submit a proposal for a follow-up PCP in a future Horizon Europe Cluster 3 Work Programme, they should ensure that the above evidence is consolidated in the project deliverables of this CSA before the submission of the PCP proposal.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

The project should have a maximum estimated duration of 1 year.

**HORIZON-CL3-2025-01-SSRI-04: Accelerating uptake through open proposals for advanced SME innovation Specific conditions**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 1.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 3.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility conditions apply: |

| | |
|---|---|
| | Consortia must include, as beneficiaries:<br>- A minimum of three (3) to a maximum of seven (7) partners.<br>- At least 2 SMEs from 2 different Member States.<br>- At least 1 end-user organisation in the areas addressed by the proposal, namely one of the following options:<br>• Option A "Fighting Organised Crime and Terrorism''<br>• Option B ‘"Disaster-Resilient Society''<br>• Option C "Resilient Infrastructure'' and<br>• Option D ‘"Border Management'', provided that the applications attain all thresholds.<br>- At least 2 Member States must be represented in the consortium.<br>Participation of non-SME industries and Research and Technology Organisations (RTOs) is not excluded, but it must be limited to 15% of the budget.<br>At least 50% of the budget must be allocated to SMEs. |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [73]. |

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Development of a mature technological solution addressing EU security policy priorities in the areas addressed by the Cluster 3 work programme;

[73] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Facilitated access to civil security market for small innovators;
- Improved cooperation between public buyers and small supply market actors for a swifter uptake of innovation in response to short to mid-term needs;
- Stronger partnerships between small and medium EU security industry and technology actors to ensure the sustainability of the EU innovation capacity in the civil security domain and reduce technological dependencies from non-EU suppliers in critical security areas.

Scope: Europe's 25 million small and medium enterprises (SMEs) are the backbone of the EU economy. SMEs can bring innovation to societal challenges, including the security of EU citizens. Innovative SMEs and high-tech start-ups can transform and modernise EU security capabilities.

However, despite the innovation capacity of EU SMEs, these often experience difficulties in finding their way to the public markets. These include red tape in public contracts, access to

new customers, access to finance, industrial competition and IP valorisation. These difficulties are exacerbated in markets that show restrictions of different kind, as it is the case of security.

Knowing that SMEs require additional support to reach the security buyers and that the collaboration opportunities offered by the projects of the Pillar II of Horizon Europe can be a catalyst for uptake, this topic aims to offer a collaborative environment for small and medium innovators to tailor their innovations to the specific needs of civil security end-users.

Applicants are invited to submit proposals for technology development along with the following principles:

- Focus on mature technological solutions addressing EU security policy priorities in the areas addressed by the Cluster 3 Work Programme;
- Fostering collaboration between SMEs from different Member States and Associated Countries;
- Involving security end-users in the role of validator and potential first-adopter of the proposed innovations;
- Fostering collaboration schemes between small companies and research and technology organisations and/or big industrial players aimed at fostering innovative technology transfer or creating innovative business models that facilitate access to market and strengthen the innovation capacity of EU SMEs and start-ups in the domain of civil security.

Examples of activities to plan in the proposed projects include, but are not limited to: assimilating market requirements; facilitating access to additional funding; approaching potential public buyers; assess competitive landscape; supporting in innovation management

(methodological and process innovation, business model innovation, market innovation); assist in IP management and exploitation; provide guidance for expansion to future markets, etc.

The participation of research and technology organisations should not focus on own technology development but on supporting the small industrial players in accelerating the technology transfer of innovative security solutions for their further development and production.

It is encouraged that one SME takes the coordinator role[74]. Exceptions to this requirement should be duly justified.

The projects should have a maximum estimated duration of 2 years.

**HORIZON-CL3-2025-01-SSRI-05: Data repository for security research and innovation**

| **Call: HORIZON-CL3-2025-01 Civil Security for Society** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 3.00 million. |
| *Type of Action* | Innovation Actions |

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Accurately gathered, stored, managed and preserved research training and testing data, disaggregated by gender if relevant, which is verified and selected in order to be realistic, up-to-date and sufficient, as well as to make research more trustworthy and reproducible;
- Researchers and projects can further increase the impact and visibility of their work by not just archiving research materials, but also opening them up for reuse and citation by other relevant actors and stakeholders;
- Properly shared and re-used relevant research data can save lives, help develop solutions and maximise the knowledge;

[74] If a MIDCAP is included in the proposal, it could also take the role of coordinator.

- Enhanced collaboration among relevant research community, improved trust between researchers and practitioners/end-users, facilitated co-operation between different research projects and reduced burden of wasted research or lost results.

Scope: The underlying idea of this topic is to avoid that security and disaster risk research projects obtain and prepare data that at the end of the projects is simply lost instead of being stored and shared for reuse.

In the security domain, due to its specificities, the special categories of data involved or/and unique limitations, which may call for additional requirements, a consolidated, common research database is particularly desired. It is of utmost importance that security practitioners are provided with an increased interoperability and improved (cross-border) exchange of data thanks to harmonised data file formats across Europe, which would easily take into account technological evolutions, i.e., be adaptable in time. Such a lack of realistic, up-to-date and sufficient training and testing data for research purposes and consequently the need for a database, data repository or any other effective and useful tool(s) to gather, manage and store varying security research data, have been regularly raised by the projects working in the area of security. The same is true of data on disaster risk management where national or regional analysis and forecasting databases or national disaster risk assessments can be fragmented or sealed without reasonable open, sustainable access to the wider community.

As a follow up of the outcomes and results of the LAGO project coming from the 2021 data topic: HORIZON-CL3-2021-FCT-01-04: Improved access to fighting crime and terrorism research data, the successful proposal, should subsequently focus on creation and deployment of a fully functional and operational common research data repository, which will extend to cover other security research areas.

The LAGO project is currently developing the skeleton of how such a repository of R&I data should be created, by providing a detailed roadmap consisting of a clear set of rules, conditions and characteristics that such a consolidated database should have. This LAGO roadmap will provide technical, legal and ethical requirements for a training and testing research data repository mostly in the area of fighting crime and terrorism, but the same project will already take into account possible applications of identified solutions in different security research domains, such as infrastructure resilience, border management or disaster resilience. The LAGO roadmap will also assess if the repository should be centralised or distributed, how to deal with "aging" data, how efficiently projects should exchange data among them taking into account security R&I specificities.

Building on the skeleton of LAGO, the newly developed data repository will enable security community (researchers, practitioners, industry, policy makers) access the scientifically satisfactory amount of up-to-date high quality and realistic data which is or was used to develop reliable (mostly digital and based on AI but also non-digital and not linked with big data) tools, technologies and solutions in support of security research and innovation. This data repository could also be very useful for verification and validation of new innovative security solutions developed under various calls in the most recent Work Programme.

Taking into account the complexity of the future repository, a multi-faceted approach will be needed and the proposal, apart from the roadmap's findings developed by LAGO, should also build on, and not duplicate, LAGO's outcomes regarding the following aspects:

- What exact types of data should be stored in the repository;
- Interoperability with existing operational systems;
- Interoperability/compatibility with European open science cloud (EOSC), with the TESSERA project[75] as well as other potentially relevant architectures and initiatives such as European Data Spaces or GAIA-X;
- How to search for data;
- Data models for security research - Harmonising of data formats;
- Concept of operations for the use of the repository by/during EU-funded security R&I projects, modalities of use, user profiles/schemes, etc.
- Legal issues, avoidance of any bias, accessibility levels related to the sensitivity of various data sets, solutions for annotation as well as for the aging of the data, etc.

The proposal should carry out extensive testing and evaluation (verification and validation), in close cooperation with ongoing projects, which would access the repository, populate it and use data intensively during the project implementation.

The proposal should develop an exploitation and sustainability plan following up the planning activities of LAGO, including funding instruments to be used for the operationalisation of the repository developed under the project as well as finding possibilities to maintain the repository after the lifetime of the project so that it not only continues to well function but is able to be extended with new data. The data repository will need to grow so it will have to be treated as an ongoing system. Co-ordination with already existing platforms or communities already using another reliable domain-specific data repository/ies for archiving and sharing research data is strongly recommended in order to verify if it would be possible to adhere in the future to a larger system or infrastructure of repositories such as European Open Science Cloud (EOSC) for example and other relevant activities.

Adopting sound security practices, such as developing comprehensive access rules to allow only authorized users with a legitimate need to access, modify, or transmit data, are crucial. Combined with a digital signature approach or multi-factor authentication, access rules go a long way in keeping sensitive data stored in a data repository secure. These and other security

[75] TESSERA project: 'Towards the datasets for the European Security Data Space for Innovation'. Internal Security Fund (ISF-2021-TF1-AG-DATA - data sets for the European Data Space for innovation).
Duration: 03/2024 - 02/2026 (24 months).

measures, such as the anonymisation of personal data, will enable the research community to fully leverage large volumes of data without introducing unnecessary security risks.

The repository developed by the proposal should preserve research data relevant to various security research domains, such as fighting crime and terrorism, infrastructure resilience, border management or disaster resilience across time and help security research community easily find, access and re-use the necessary data. The development and the functioning of the repository will be based on the outcomes of the roadmap from the LAGO project[76] from 2021 FCT call project within the remits of Horizon Europe regulation (including ethics). The repository should be operational to be tested for at least one year before the project ends. Data sharing will be based on open science principle of 'as open as possible, as closed as necessary'. Particular efforts should be made to ensure that the data produced in the context of this topic is FAIR (Findable, Accessible, Interoperable and Re-usable). To make data FAIR, the basics of good Research Data Management will have to be applied.

All necessary system features as well as the functioning of the repository should comply with privacy and data protection requirements when handling data, in order to facilitate data management ensuring full access to the data actually needed (in line with the necessity and proportionality principle and in full respect of fundamental rights and applicable legislation.

Projects should take into account, during their lifetime, relevant activities and initiatives for ensuring and improving the quality of scientific software and code, such as those resulting from projects funded under the topic HORIZON-INFRA-2023-EOSC-01-02 on the development of community-based approaches.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

The project should have a maximum estimated duration of 3 years.

[76] https://lago-europe.eu/

## Other actions not subject to calls for proposals

### 1. External expertise for reviews of projects

This action will support the use of appointed independent experts for the monitoring of actions (grant agreement, grant decision, public procurement actions, financial instruments) funded under Horizon Europe and previous Framework Programmes for Research and Innovation, and where appropriate include ethics checks, as well as compliance checks regarding the Gender Equality Plan eligibility criterion.

Form of Funding: Other budget implementation instruments

Type of Action: Expert contract action

Indicative budget: EUR 0.62 million from the 2025 budget

### 2. Workshops, conferences, experts, communication activities, studies and innovation uptake promotion

- Support to workshops, expert groups, communications activities, or studies. Workshops are planned to be organised on various topics to involve end-users (e.g. the Community for European Research and Innovation for Security); preparation of information and communication materials, etc.
- Organisation of cybersecurity conferences and support to other cybersecurity events; socio-economic studies, impact analysis studies and studies to support the monitoring, evaluation and strategy definition for cybersecurity and digital privacy policy.
- Support to promotion of innovation uptake, including through supporting developing certification testing methodologies for innovative technologies.

Form of Funding: Procurement

Type of Action: Public procurement

Indicative budget: EUR 1.47 million from the 2025 budget

## Budget[77]

| | Budget line(s) | 2025 Budget (EUR million) | 2026 Budget (EUR million) |
|---|---|---|---|
| **Calls** | | | |
| HORIZON-CL3-2025-01 | | 140.50 | |
| | *from 01.020230* | *140.50* | |
| HORIZON-CL3-2025-02 | | 90.55 | |
| | *from 01.020230* | *90.55* | |
| Contribution from this part to call HORIZON-MISS-2025-01 under Part 12 of the work programme | | 2.29 | |
| | *from 01.020230* | *2.29* | |
| Contribution from this part to call HORIZON-MISS-2025-03 under Part 12 of the work programme | | 2.59 | |
| | *from 01.020230* | *2.59* | |
| Contribution from this part to call HORIZON-MISS-2025-04 under Part 12 of the work programme | | | 1.36 |
| | | *from 01.020230* | *1.36* |
| Contribution from this part to call HORIZON-MISS-2025-06 under Part 12 of the work programme | | | 0.23 |
| | | *from 01.020230* | *0.23* |
| Contribution from this part to call HORIZON-MISS-2025-05 under Part 12 of the work programme | | 2.48 | |
| | *from 01.020230* | *2.48* | |
| Contribution from this part to call HORIZON-MISS-2025-07 | | | 0.11 |

[77] The budget figures given in this table are rounded to two decimal places.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for 2025.

| | | | |
|---|---|---|---|
| under Part 12 of the work programme | *from 01.020230* | *0.11* | |
| **Other actions** | | | |
| Expert contract action | | 0.62 | |
| | *from 01.020230* | *0.62* | |
| Public procurement | | 1.47 | |
| | *from 01.020230* | *1.47* | |
| Contribution from this part to Indirectly managed action under Part 12 of the work programme | | 0.61 | |
| | *from 01.020230* | *0.61* | |
| Contribution from this part to Specific grant agreement under Part 12 of the work programme | | 0.78 | |
| | *from 01.020230* | *0.78* | |

| | | | |
|---|---|---|---|
| Contribution from this part to Public procurement under Part 12 of the work programme | | 0.45 | 0.04 |
| | *from 01.020230* | *0.45* | *0.04* |
| Contribution from this part to Provision of technical/scientific services by the Joint Research Centre under Part 12 of the work programme | | 0.01 | |
| | *from 01.020230* | *0.01* | |
| Contribution from this part to Expert contract action under Part 12 of the work programme | | 0.03 | |
| | *from 01.020230* | *0.03* | |
| **Estimated total budget** | | 244.08 | 0.04 |